Beliefs and attitudes of citizens in Germany towards smart surveillance and privacy

Noellie Brockdorff[1], Natalie Mundle[1], Christine Garzia[1], Thomas Wilkening[2]
[1] Department of Cognitive Science, University of Malta, Msida, Malta
[2] Georg-August-Universitaet Goettingen Stiftung Öffentlichen Rechts, Goettingen, Germany

December 2013

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285582.

SMART
Scalable Measures for Automated Recognition Technologies (G.A. 267127).
The project was co-financed by the European Union within the Seventh Framework Programme (2007-2013).
https://www.smartsurveillance.eu/

Correspondence about this report should be addressed to
Noellie Brockdorff, Department of Cognitive Science, University of Malta, Msida, MSD2080, Malta
noellie.brockdorff@um.edu.mt

Table of Contents

1. Key Findings

This document presents the German results of a qualitative study undertaken as part of the SMART project – "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727). The analysis and results are based on a set of three focus group discussions comprising of 22 participants, which were held in order to examine the beliefs and attitudes of citizens towards smart surveillance and privacy.

The focus group discussions were conducted in line with a discussion guide mainly consisting of different scenarios aimed at stimulating a discussion amongst the participants. While some scenarios dealt with surveillance in everyday contexts likely to be encountered by research participants, other scenarios were hypothetical in nature and their aim was to elicit the feelings, beliefs and attitudes of the participants in relation to dataveillance, the massive integration of data from different sources, and the "security versus privacy trade-off".

The German participants were in general highly aware of being under surveillance in different contexts including commercial, boundary and public spaces. When discussing these contexts, a wide range of surveillance technologies and methods was mentioned, including the use of loyalty cards in order to monitor customer behaviour and the use of CCTV systems for the observation of citizens. Overall, participants perceived customer surveillance as taking place mainly for security, marketing and advertisement purposes, while they perceived general citizen surveillance as occurring for reasons of national security and personal safety. Most participants were also aware of the extent of surveillance and its pervasiveness when using a mobile device, and strongly questioned their privacy since they appeared particularly concerned regarding the sharing of citizen data between third parties.

In order to gauge participants' attitudes and beliefs on integrated dataveillance, the group was presented with a fictional scenario illustrating the massive integration of data. After an initial intense reaction to this situation by the majority of participants, the possibility of massively integrated dataveillance actually occurring was debated from both from a technical and legal perspective. Even though opinions varied, from a technical point of view the majority of participants considered the massive integration of personal data as either currently possible, although not to the extent as portrayed in the scenario, or else regarded it as an impending possibility. On the other hand, from a legal perspective, most participants perceived the occurrence of dataveillance as being unlikely due to current legal restrictions; however some participants argued that future legal developments could not be excluded. Nevertheless, the majority of participants showed disbelief that the state or related agencies could have any interest or time to deal with citizens' extensive personal details, although a minority of participants did refer to the extensive spying measures taken by the state during the times of the German Democratic Republic.

Participants' opinions on the effectiveness of smart surveillance from a security aspect varied, particularly those in relation to the autonomous decision-making capabilities of smart technologies. While some participants argued that automatized systems are more efficient in comparison to those requiring a human operator, whom they perceived as likely to be distracted or influenced by biases, others appeared to be sceptical and distrustful of technology on its own without human agency. Overall, these participants disputed the use of fully automated surveillance technologies and instead advocated the inclusion of the human element in surveillance.

During the discussion of the "security-privacy trade off" scenario, it appears that the use of video-surveillance in public places was generally accepted since such use was perceived as reducing criminality. In contrast, most participants showed a hostile attitude towards sound sensors, biometric technologies, and electronic tagging. It appears that, with the exception of CCTV systems, any increase in surveillance measures was perceived as posing a threat to citizens' safety through the increase in risk of data theft and misuse as well as resulting in a violation of privacy, a restriction on freedom, and having a chilling effect. As a result, most participants rejected the idea that an increase in surveillance would result in increased personal safety and public security. In general they argued that surveillance could not solve the problem of violence and that security could never be fully guaranteed, with only a minority arguing in favour of an intensification of surveillance measures following an increase in crime.

Participants were also invited to share their viewpoints on surveillance laws and regulations. Participants showed a general lack of knowledge with regards to the legislation, which they partly attributed to their own lack of initiative as well as on the difficulty of understanding legal jargon. In relation to the effectiveness of legislation, opposing views were evident; while some participants regarded current legislation as inadequate, others conveyed their satisfaction with the level of protection offered. Additionally, in relation to the length of storage of surveillance data, expectations were varied and while some participants appeared indifferent regarding storage period, others seemed concerned regarding the management of and access to the stored surveillance data. Lastly, vis-à-vis the sharing of data, while in general this was perceived as acceptable between state authorities, albeit not in an unrestricted manner, participants expressed their unease with respect to data sharing amongst private entities.

2. Introduction

The analysis and results in this document are based on a set of three focus groups carried out in order to gauge the attitudes of citizens towards smart surveillance and privacy. This research was undertaken as part of the SMART[1] project.

The University of Malta as Work Package Coordinator was responsible for the design of the research materials, methodology, and coordination between partners, data analysis and report writing. The SMART project partners in each country were responsible for the translation and back-translation of the research materials, recruitment of participants, recruitment and briefing of moderators, conducting the focus groups, transcription of the discussions, and translation of transcripts into English. The SMART project partners for Germany are Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts (UGOE) and Gottfried Wilhelm Leibniz Universität Hannover (LUH).

Focus group discussions were conducted in a total of 14 countries and this document provides the findings from the study that are relevant to Germany. Other separate reports are available for Austria, Bulgaria, Czech Republic, France, Italy, Malta, Norway, Romania, Slovakia, Slovenia, Spain, the Netherlands and the United Kingdom.

The following table provides a breakdown of the participants according to country, age and gender:

Country	Group 1 (18-24 years)		Group 2 (25-44 years)		Group 3 (45+ years)	
	M	F	M	F	M	F
Austria	2	4	3	4	4	2
Bulgaria	6	6	5	5	2	6
Czech Republic	4	6	4	5	4	5
France	5	4	5	4	5	5
Germany	1	6	4	3	4	4
Italy	1	5	3	3	2	7
Malta	5	5	4	6	3	5
Norway	3	6	4	3	2	5
Romania	6	1	3	4	2	4
Slovakia	7	6	5	5	5	5
Slovenia	5	5	5	3	6	4
Spain	6	5	6	3	3	5
the Netherlands	2	4	6	2	4	4
United Kingdom	4	2	5	3	5	4
Sub-total	57	65	62	53	51	65
Total	**122**		**115**		**116**	

[1] "Scalable Measures for Automated Recognition Technologies" (SMART; G.A. 261727) – which was co-financed by the European Union under the Seventh Framework Programme for Research and Technological Development of the European Union (SEC-2010-6.5-2. "Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules").

3. Methodology

In total, 42 focus groups – three in each country – were conducted between February and November, 2013. Thirty-nine of the groups had between 6 and 10 participants, three groups had 11, 12 and 13 participants respectively. Overall, 353 participants took part in this research project. The focus groups in Germany were carried out on the 18th, 19th, and 20th February 2013. The composition of the groups held in Germany is described further on in Section 4.

Personal references and snowball techniques were used in order to recruit participants willing to take part in this study which does not claim to be necessarily representative for the entire EU population or any of the individual EU countries where focus groups were conducted.

3.1 Recruitment process

As illustrated in the table above, three focus groups were conducted in each country which were composed of participants from the following age groups:

- Group 1: 18-24 years
- Group 2: 25-44 years
- Group 3: 45+ years

A number of selection criteria were recommended with regards to the recruitment of the focus group participants and therefore all potential participants were asked to fill in a recruitment questionnaire (see Appendix A). While the recruitment of an equal number of males and females was recommended, it was also desirable to recruit participants with a diverse educational level and occupational status. Effort was also made in order to recruit participants residing in different locations (city, town and rural area). Moreover, in order to be recruited, it was suggested that participants should be exposed to a number of surveillance applications and technologies in their everyday life. Although such recommendations were suggested, the fulfillment of all these criteria proved rather challenging during the recruitment process.

It should also be noted that during the recruitment process, potential participants were not provided with detailed information about the topic of the focus group. They were solely told that the discussion would be on the topic of "technology and privacy". This was done in order not to influence or bias the discussion.

3.2 Discussion guidelines

Discussion guidelines (see Appendix B) were developed with the aim of gauging citizens' awareness and understanding of smart surveillance technologies and also at gaining an in-depth understanding of citizens' beliefs and attitudes towards smart surveillance and privacy. The discussion guidelines were developed and further refined following a pilot study conducted in November 2012. The discussion guidelines were designed to tackle the main themes under study through a variety of scenarios. While

some scenarios dealt with surveillance in everyday contexts likely to be encountered by research participants, other scenarios were hypothetical in nature and their aim was to elicit the feelings, beliefs and attitudes of the participants in relation to dataveillance, the massive integration of data from different sources and the “security versus privacy” trade-off.

The discussion guidelines were translated into each national language where the research was conducted. Moreover, back translations were carried out which entailed an independent translation of the discussion guidelines back into English by a different translator. The back translation was then compared with the original version in order to ensure comparability of meaning and clarify any possible discrepancies. Any possible changes were discussed with the partners, and, where relevant, the necessary amendments were carried out until a final version of the discussion guidelines in the national language was approved. The German version of the discussion guidelines can be found in Appendix C.

3.3 Focus group procedure

The focus groups were conducted by a team consisting of a moderator and an assistant moderator. In certain cases, other team members were present in order to assist with logistics and other tasks including taking notes during the discussion and filling-in a de-briefing form (see Appendix D) at the end of each session.

All participants were required to read and sign a consent form (see Appendix E) prior to their participation in this study. The participants were informed that everything that is recorded during the session will be kept confidential and that their identity will remain anonymous. The moderator also informed the participants that they will be assigned a number each and that only this number will be used in the report.

All focus group sessions, which were audio-recorded in order to be transcribed, were conducted in the local language. In general, the duration of the sessions was between one and a half to two hours. Following the end of the session, some partners opted to offer incentives for participation including monetary remuneration or the provision of tokens such as book vouchers. Additionally, those participants who were interested in the research were given more information about the SMART project.

3.4 Data analysis

After conducting the focus groups, all sessions were fully transcribed in the local language and subsequently translated into English. The de-briefing forms were also translated into English. The coding process was carried out by three researchers and was based on 3 different data sets (the English transcripts from Austria, Czech Republic and Italy). An initial coding structure was developed through the process of coding and re-coding as the transcripts were read and interpreted. Such a process initialised a critical recategorising and rethinking of the codes first applied, and allowed for a more

focused data analysis and drawing together of overarching themes. Thus, the initial coding map was modified as the analysis unfolded. This process of revision was concluded once no new themes emerged and a final coding map was agreed upon. Nevertheless, the emergence of additional lower order codes was not excluded since the analysis of the remaining transcripts was still pending at this stage. The coding map for this report can be found in Appendix F.

Further to the above process, the researchers proceeded to analyse the remaining 11 data sets. Draft versions of each country report were prepared and provided to the respective partner for revision and amendments.

4. Description of the Sample

The data analysis for Germany is based on 22 participants. In general it was noted that it was rather difficult to find participants willing to attend the different focus groups. Moreover, some participants also failed to show up on the day, despite two reminders being sent out, one a week prior to the focus group and another one on the day of the focus group.

The composition of all three groups is depicted in the following table:

Participant number	Group 1 – 18-24 years	Group 2 – 25-44 years	Group 3 – 45+ years
P1	F	F	F
P2	F	M	M
P3	F	M	No-show
P4	No-show	F	M
P5	F	F	M
P6	M	No-show	No-show
P7	F	M	F
P8	No-show	M	F
P9	F	No-show	F
P10	No-show	No-show	M
Total	**7**	**7**	**8**

A number of differences in the group dynamics and in the flow of the discussion were evident in the three groups. In Group 1 (18-24 years), although the atmosphere was described by the moderators as friendly and cordial, the group participants were also rather formal. Participants were generally cooperative and no one was particularly aggressive or noisy. The discussion was smooth but not very free-flowing with the exception of one or two situations. It appears that some questions were not very well understood by the group participants.

In comparison to Group 1, the atmosphere in Group 2 (25-44 years) was more intense, especially during certain instances of the discussion. However, most of the time participants were friendly, cordial, cooperative and engaged well with the discussion. However, in a few situations, especially when one or two participants had different points of view, the moderators observed that the tone of the discussion became more heated. Although the discussion started off as rather free-flowing, overall the discussion was described by the moderators as not particularly smooth. Due to some situations when participants disagreed with each other's opinion on a couple of issues, the discussion was a bit more heated and confrontational in comparison to the Group 1 discussion. Unfortunately, these animated discussions did not necessarily deal with the core topics of interest.

The third and final focus group (45+ years) was described by the moderators as being more noisy and aggressive than the previous groups. At the beginning, the atmosphere was mostly cordial and friendly; nevertheless, in this group, the discussions and arguments were noticeably more intense and slightly aggressive compared to the previous two groups. According to the moderators, the strong arguments of two participants (P4 and P7) might have slightly intimidated some of the others. The discussion in

general was described as free flowing and the participants were engaged and some were particularly enthusiastic, unfortunately not necessarily concerning the topics that were on the agenda. In fact, the moderators stated that they found it very difficult to stick to the relevant questions and topics. Moreover, the moderators had the impression that some participants already had certain opinions on any topics which they wanted to contribute, regardless of the relevant question at the time. As a consequence, the discussion became rather difficult to lead and in some situations it was confrontational and heated. In this older age group which was mostly composed of elderly participants, some participants showed less respect towards the moderator, co-moderator and the basic rules, possibly because of the age difference.

5. Results

5.1 Surveillance Technologies in Different Spaces

In order to establish what the focus group participants actually knew about different surveillance technologies in different spaces – who is collecting what types of information, where and for what purpose – they were asked to imagine everyday situations like being in a supermarket, in an airport whilst travelling, visiting a museum, participating in a mass event such as a football match or concert, and simply using their mobile phone.

5.1.1 Commercial Space

In commercial spaces, specifically in the context of a supermarket, participants in all three focus groups generally displayed a high awareness of being surveilled: "*I do not think that I am monitored – I know it for a fact*" (P7-III). Participants in all groups mentioned a number of surveillance measures in commercial spaces, namely loyalty cards, CCTV and financial monitoring.

The predominant method through which participants felt surveilled was via loyalty cards, the main purpose of which was perceived to be the collection of personal data. In addition, loyalty cards and CCTV were seen to record customers' shopping behavior, which was believed to be utilised for market research with the ultimate aim of enhancing the shelf and product organisation of commercial establishments. It appears that most participants expressed a certain level of mistrust towards the use of loyalty cards which appears to stem from the belief that the exclusive benefits linked to their use are solely provided in order to tempt customers into providing their data: "*I think the bonus system is just a bluff to get information about the consumers' behaviour*" (P4-II). In addition to the collection of data, participants also believed that the data was sold to various third parties; more specifically they presumed that product manufacturers and institutes for market research were interested in their data, which they would purchase from supermarkets.

The second most frequently mentioned surveillance measure in commercial spaces was CCTV, which was regarded by some participants as a *"standard"* (P6-I) feature in commercial establishments. In addition to perceiving video-surveillance as having a security function, primarily in relation to theft prevention, some participants argued that video-surveillance is additionally employed by businesses for the observation of consumer behaviour:

> *"[…] However, I think the video recordings are also used for analysing [customer behaviour], not only for theft prevention: what can we put where? Where do people walk around? How do they walk? And the market's interiors are being re-arranged all the time, to force the customer into having to re-orientate again and again, and I think this is made for that purpose, too" (P9-I).*

In addition, participants mentioned the financial monitoring of customers in commercial spaces through the collection of bank card details: "*I am convinced that some companies save my purchases especially when I pay by electronic cash card*" (P1-II). It appears that some expected this to occur not only by private companies, such as supermarkets, but also by the state. Moreover, albeit to a lesser extent, some participants also mentioned the use of RFID-tags on products as another method of surveillance. In relation to this, participants believed such devices as being useful for tracking stolen items or for tracking items which are purchased by a suspicious person.

Lastly, surveillance was also regarded as occurring through the deployment of private detectives and security personnel, as well as via the use of mirrors on ceilings; such methods were mainly perceived as being employed for the prevention of theft and crime.

5.1.2 Boundary Space

In the context of border control in spaces such as airports, the discussion mainly focused on an airport setting as a boundary space, while, to a much lesser extent, surveillance at land borders and on highways was also briefly discussed. The pervasiveness of surveillance in airports was evident, with participants sharing their impression of being "*monitored automatically*" (P2-III) by various surveillance measures when entering such a space. Such measures included passports checks, physical screening by security agents, as well as the investigation of travellers' luggage content for the detection of suspicious objects with machines using x-rays or scanners.

Most focus group 3 members (age 45+) expressed their mistrust in surveillance measures, which they regarded as being primarily used for the observation of people and less for safety reasons and therefore claimed to live in a "*surveillance state*" (P4-III). However, it appears that other participants perceived these surveillance measures as necessary for purposes of national security, more specifically for the prevention of crime, terrorism and illegal immigration as well as for the tracking of criminals. In view of such reasons, participants conveyed their general acceptance of such measures: "*You cannot withdraw from this surveillance. But it does not feel too bad to me since it is also for protection. And that is very important. So for travelling, 'surveillance' is the wrong word*" (P7-III).

In addition to the aforementioned purposes, surveillance was also believed to occur for reasons relating to customs affairs, more specifically in order to ensure that duty and taxes were paid by passengers. Further purposes mentioned were those concerning organisational and marketing functions. Consequently, participants expected public and private parties with national and international interests to be involved in surveillance measures at airports. Data sharing among these entities and data selling to third parties for the enhancement of business was expected. Moreover, bonus cards for the collection of flight miles were regarded as being utilised for reasons similar to the use of loyalty cards in supermarkets with the difference that, in this case, such monitoring was aimed at analysing travellers' behaviour.

It appeared that some participants perceived a number of differences between surveillance measures at European airports and those used in foreign airports, particularly in the United States. Personal checks when travelling to the U.S. were experienced to be more intense compared to other countries, because travellers had to allow U.S. authorities to what they considered was extensive access to their data before travelling: "*Especially if you travel to the United States, there you really have to reveal everything and you are surveilled universally*" (P2-I). In this regard, some participants expressed their belief that travellers have no choice regarding the disclosure of their data, and proceeded to argue that such procedures limit citizens' "*freedom to travel*" (P8-II).

5.1.3 Common Public Spaces

In common public spaces, specifically at large public events such as sport games, demonstrations and concerts, and also in public institutions such as museums and libraries, participants expressed their awareness of several surveillance measures, including CCTV, law enforcement personnel and security guards, which were perceived as '*ubiquitous*' (P2-III).

In relation to monitoring measures undertaken in public or private places hosting large crowds, it appears that surveillance has undergone a process of normalisation. In general, it seems that participants were not only accustomed to surveillance in this space but that they actually expected a certain amount of security measures to be taken at large mass gatherings: "*I expect some kind of surveillance at every large event for the safety of public property and myself*" (P2-II). Rather than being directed at every individual present, such surveillance was perceived as targeting specific individuals: "*I do not think that they [arbitrarily] choose a person [to observe], but there might be a certain profile that they are looking for and they only search for individuals that match this profile*" (P1-II).

Moreover, the presence of law enforcement personnel with cameras at demonstrations and large sports events was widely accepted by participants. It appears that they expected such monitoring to have two main functions: firstly they perceived this as having a deterrent effect, and, secondly, they argued that video-surveillance data could prove useful for the investigation of crimes. Nevertheless, some participants also expressed the belief that excessive police presence at large events is exaggerated and, in such cases, they suspected the state of possibly monitoring citizens' political opinions during demonstrations.

In addition, further mistrust into the nature of surveillance being purely for security reasons was expressed by participants who believed that for event organisers, commercial motivations played a strong role because many private companies were involved in such organisation:

> "*I think that at concerts, this is some kind of pseudo-security. For example at the entrance they check your bag because they do not want you to bring any food into the localities, so that they can sell their own food. So this is not for security reasons*" (P1-III).

Apart from debating surveillance at large events, participants also discussed the use of surveillance in other public spaces such as museums and libraries. First and foremost, participants mentioned the use of CCTV for the protection of property, more specifically for the prevention of vandalism and theft. The collection of personal data was also discussed in this context and although participants mentioned the collection of visitors' data, they expressed uncertainty as to the use of such data. In general, it appears that participants perceived the aforementioned surveillance measures in the public space as justified, and hence as acceptable.

5.1.4 Mobile Devices and Virtual Spaces

The majority of participants expressed the opinion that surveillance in this space is pervasive: "*Everything is being watched*" (P4-II). In relation to this, several participants differentiated between the surveillance potential of *"classic cell phones"* and that of smartphones: *"[…] with the smartphones I guess the spectrum is a lot wider* (P3-I). Similarly, another participant argued that the use of smart phones has considerably increased privacy risks:

> "*The more technology advances, the more it infringes our privacy, one can see that with the smart phones. 10 years ago, data was much safer, because there were not so many devices having access to it" (P9-I).*

Participants mentioned a number of surveillance possibilities via the use of mobile telecommunication devices, including location tracking via GPS, monitoring of call lists and data traffic and even the possibility that phone conversations could be recorded:

> *"[…] I use my smart phone* 24/7*, too. I want to add that one is surveilled everywhere, with everything that is doable with the cell phone, whether it is email traffic, conversations or SMS, I think that all can be captured intercepted, used, the whole data about where you currently are […]"(P1-I).*

As the above quote illustrates, participants seemed to be rather knowledgeable about the technological surveillance of mobile phone data and the ubiquity of surveillance through the use of such devices, especially through the variety of functions offered by smartphones. Participants expected a variety of data to be collected and shared amongst the commercial parties involved, such as network providers, mobile phone manufacturers, and private companies providing web search engines; consequently, participants questioned the protection of their privacy:

> "*The network providers give us the abstract idea of us having privacy. However, all information that goes through the smart phone also goes to every website interested in the data. [...] Every agency which is allowed to have the data also wants to have it. I think with smart phones everything that I type or speak is revealed" (P2-II).*

Although participants appeared to believe that their data could not be passed on to third parties without their consent, they increasingly raised doubts about what companies actually do in practice: "*Everything I click on, what I like, where I want to be, how often I use it, where I am and what I use is passed on without me knowing*" (P5-II). Participants specifically assumed that secret services, such as the Federal Intelligence Service in Germany, had unlimited access to their data if it was shown to be useful in the context of crime prevention or investigation. In particular, focus group 3 (45+ years) participants showed their mistrust towards spying activities of the state, referring to a specific case of historical surveillance in times of the German Democratic Republic (GDR) when the State Security Service (Stasi) secretly surveyed citizens excessively. As one participant stated, there are possibly no limits to state surveillance:

> "*Yes we now live in the Federal Republic, but I do not think that this is another state model. Talking about these institutions, you can be absolutely sure that there is no difference between socialism and capitalism. It is just a surveillance apparatus. Every state has it and they will research what they want" (P4-III).*

Lastly, apart from the state granting itself the right to access personal data, participants also feared security leaks when connecting to unsecured Wi-Fi with a computer or smart phone and when using smart phone applications because in their opinion "*everything can be spied on by strangers*" (P2-I).

5.2 Perceptions & Attitudes towards Smart Surveillance and Integrated Dataveillance

One of the central tasks of this study was to research citizens' feelings and beliefs towards smart surveillance and massively integrated dataveillance, the latter referring to "*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*"[2]. In order to tap into the attitudes of the participants, the group was presented with an everyday scenario: a recorded telephone conversation between a job seeker and a civil servant of the employment agency, where complex surveillance[3] becomes evident.

5.2.1 Feelings

After having listened to this conversation, the focus group participants revealed a wide range of feelings including extreme discomfort, anger, fear and disbelief. In contrast, very few participants expressed positive feelings, mainly due to the consideration that such a situation could, to a certain extent, be convenient.

In general, strong negative reactions to this *"frightening"* (P5-I) scenario were expressed throughout all focus groups, including feeling "*uncomfortable*" (P3-I), "*uneasy*" (P4-II), "*shocked*" (P3-I) and *"speechless"* (P5-II). The mere idea of extensive surveillance measures caused participants to feel "*anxious and insecure*" (P3-I) due to a feeling of being exposed and violated: "*I would feel that my personal life would be infringed*" (P4-II). To a lesser extent, reactions of complete rejection were expressed specifically by focus group 3 participants, who considered this as a *"dreadful"* (P1-III) idea: *"Well, I'd be horrified, really! Simply horrified!"* (P8-III). Lastly, expressions of indignation and anger also resulted amongst the participants: "*I would be extremely angry and the manager would have serious problems with me*" (P2-II).

In contrast to the majority, a very few participants expressed positive feelings. In this case, they primarily regarded surveillance as providing them with a sense of comfort and convenience: "*I would feel like someone is looking after me and it would be well appreciated, because it would mean less hassle*" (P2-III). Similarly, another participant welcomed what he perceived as an enhanced service by public authorities: "*There would be no need to bring documents to the departments, which would be great*" (P6-I).

5.2.2 Behavioural Intentions

[2] Clarke, R. (1997).

[3] The statements of the civil servant allude to a drawing together of the job seeker's personal information from various public and private databases, health-related information, bank / credit card data, surveillance of online social networks, and CCTV. See Appendix B, Item 4 for full text of scenario.

In addition to asking about their feelings, participants were also asked for their resulting behavioural intentions. In general, it appears that those participants who conveyed feelings of discomfort and anger revealed a need to understand how it was possible to collect all this data about citizens and thus expressed an intention to investigate: "*I would try to calm down and understand how they know these things about me and if there are any possibilities to make them stop*" (P3-I). Furthermore, the majority of participants, perceiving the scenario as unacceptable, shared their intentions of counteracting such a massive integration of data: "*I would do anything if this happened to me to prevent it from happening to me again*" (P1-III).

Additionally, other participants declared that they would resort to legal action by investigating the legitimacy of the situation: *"I would study the law and then take legal measures*" (P8-II). Others stated that they would directly confront the state to clarify the situation: "*My reaction would be to go to the Supreme Constitutional Court and ask to know why the state collects so much data about me and what they are using it for*" (P6-I). By expressing such intentions, it appears that these participants revealed a certain faith in the existing legal system and protection by law. Moreover, to a lesser extent, some participants perceived such an occurrence as a failure of the organisation and stated they would file an organisational complaint: "*I would contact the account manager [...] I do not agree [with] or accept something like that*" (P3-II).

Passive reactions were rather rare amongst the participants and it seems that an immediate withdrawal from the situation, such as hanging up, was expressed by very few participants: "*I would hang up the phone and then I do not know*" (P2-II). Such passive reactions appear to reflect the helplessness of these participants. Additionally, others expressed their wish to escape from public exposure in order to protect themselves: "*The first instinct you get is to shut yourself off from everything by staying at home and doing nothing at all*" (P3-I).

5.2.3 Beliefs

5.2.3.1 Likelihood of smart surveillance and integrated dataveillance

Regarding the likelihood of whether or not smart surveillance and massivley integrated dataveillance are possible and realistic (currently and/or in the future), the focus group participants generally distinguished between technical and legal aspects.

From a technical point of view, the majority of participants perceived such a scenario as either currently possible, although not to the extent portrayed in the scenario, or else considered it as an impending possibility: *"I think it's exaggerated but I keep thinking if something like this would be possible in the near future"* (P9-III). In this regard, some participants, albeit in a slightly hesitant manner, considered this possibility as being dependent on the extent of technological development: "*If the technology advances fast, it will be possible soon. Or it is possible now, but we do not know it*" (P3-II). Furthermore, some participants argued that as soon as the available data could be centrally organised with an

advanced technological system, the scenario would become a concrete possibility: "*I really think this is possible because the data is there and it just needs to be integrated*" (P1-III). On the other hand, others did find the massive integration of data as difficult to conceptualise: "*This goes far beyond my imagination*" (P2-II).

Nevertheless, from a legal perspective, the majority of the participants considered the local legal context as presenting an obstacle to extensive surveillance. More specifically, they expected the state to regulate the collection and use of data in a firm manner:

> "*Of course data can be collected. But I think a scenario like this is kind of imaginary, because the collection and use of data is governed and monitored by the state with strict guidelines and laws, which determines what is legal and not*" (P6-I).

On the other hand, some participants argued that future legal developments could not be excluded: "*If the law would allow that the data is linked then it is going to happen. So far it is not like this, but it will be one day*" (P7-II). Overall, while most participants revealed their trust into the protective measures of the state, a minority of participants expressed their mistrust towards the protection of citizens' privacy by the state and expected the integration of their data to be "*definitely possible, even if it is not legal. [...] we cannot know for sure*" (P2-I).

Nevertheless, regardless of the above views debating both technical and legal aspects, it appears that several participants questioned why the state and its agencies would want to be in possession of such extensive personal details of citizens' lives. They thus regarded the scenario as unrealistic: "*I do not think any department would have an interest in data like this. [...] They do not need it for their work*" (P9-I). In contrast, a number of focus group participants from group 3 (45+ years) expressed their suspicion towards the state, given that they could clearly imagine a reproduction of the extensive spying measures which were taken during the times of the German Democratic Republic.

5.2.3.2 Acceptance of smart surveillance and integrated dataveillance

Overall, it appears that the opinions of most participants were rather mixed and that their acceptance of massively integrated dataveillance depended on several criteria including the type of data collected, by whom it was gathered, and also the purpose of collection. Another important decisive factor for the participants was whether their data was subsequently shared with other parties and whether they were explicitly asked for their consent.

Notwithstanding these different criteria, it appears that the main criterion for the acceptance of dataveillance was the type of data collected. Albeit participants' opinions in this regard were diverse, the majority of participants agreed upon the acceptability of sharing a minimum amount of personal data, which they defined as the data on one's identity card and also the basic personal details one has to share in order "*to exercise [one's] right to vote*" (P2-II). Some stated that they regarded the act of

sharing one's "*basic data*" (P7-III) as normal, providing it without any hesitation: *"[…] one gets used to exposing it nowadays"* (P7-III).

However, the majority of participants were of the opinion that they "do *not see any point"* (P7-I) in sharing more data than one's basic personal information. In particular, it seems that the sharing of contact details was perceived as uncomfortable by most participants because of the increased probability of being subjected to marketing phone calls or of receiving spam e-mails. Additionally, participants specifically discussed the sharing of their financial and health data, which they generally considered as unacceptable, as well as the collection of other data, including religious beliefs and sexual orientation, which they considered as being extremely sensitive: "*I think this is data that is so private that even the state should protect it stronger than other data, so others cannot use it"* (P1-I). On the other hand, in stark contrast to the opinions of the majority, one participant in a rather frank manner expressed his willingness to spread his personal data as much as possible and on purpose: "*The more I scatter my data the less it is valuable*" (P8-II).

On a last note in relation to the sharing of data, it appears that participants, especially those in Group 1 (18-24 years) expressed two main points of views with regards to the extent that individuals are in control of what actually happens to their data. Firstly, some participants conveyed a sense of helplessness due to the belief that they have no control whatsoever:

> *"I feel affected all of the time, when data is collected about me, no matter which method is used […] I do not know, where my data is and nor do I have control about it at all. Especially with data collected without me consenting to it. I feel anxious about this" (P2-I).*

On the other hand, despite the lack of control as expressed above, it appears that others, albeit acknowledging that having total control is unrealistic, did feel more in control about which data they consented to be shared or not, and regarded it mainly as part of a citizen's self-responsibility:

> *"Most of the time you are aware which data you share; you consent. Okay, maybe when you get instructed about the data protection regulations and opt in, that you have read them, [while in truth] you have not [actually] read them. But then again you have to blame yourself for that, for sharing everything, and then you should not be angry or wonder. But of course there are things that happen in the background, without you noticing it. Where data is collected, shared, used" (P1-I).*

5.2.3.3 Perceived effectiveness of smart technologies and dataveillance

When discussing the effectiveness of surveillance technologies, participants differentiated between traditional surveillance technologies, in which case it was perceived that human judgement is necessitated in decision-making, and smart technologies, in which case it was perceived that decisions are taken by a computer programme.

Primarily, it appears that participants were keen to challenge the automatic decision-making process by a machine and more specifically questioned whether machines have the ability to take circumstantial aspects into consideration. In particular, some participants appeared concerned regarding the likelihood that certain actions could be misunderstood:

> "*I think that an automatic detection of dangerous situations involves the danger that [for instance] when I make a movement, the system interprets [this movement] incorrectly and that I will get raided by policemen or who knows what*" (P1-III).

In addition to the possibility of misinterpretation, several participants seemed uneasy with the idea that the accuracy of a machine judgement could be taken for granted; in their opinion, the risk of inaccuracy was higher. As mentioned previously, these participants felt uncomfortable with a decision making process devoid of the human element: "*I still want that, in the end, a person decides because I think that intellect and emotions [are important], [and] no technology can compensate this*" (P7-III). Moreover, participants believed in the inability of machines to discriminate without considering all aspects of the situation as well as the individuality of a person's behavioural traits. This was perceived by some as leading to a sense of dehumanisation:

> *"It is a problem, that you are more an object than a human, when monitored with new surveillance methods. You are not getting analysed, not everything is taken into account, there is only generalisation, you get categorised and that´s it" (P1-I)*.

One participant in particular regarded the programming of smart technologies as being based on the "*standardization*" (P7-III) of human behaviour and appeared concerned that citizens could potentially be arrested for "*behaving differently*" (P7-III). However, in spite of the criticisms leveled at the automatic decision-making process of smart surveillance, the human element was also subject to debate. In particular, some participants stated their preference for an automatised decision-making process, arguing that human operators have the tendency to be influenced by their biases: "*A machine does what it should do. So I would [have] trust in machines more than in human beings*" (P2-II).

Another aspect discussed in relation to effectiveness was the perception that, due to their automated nature, smart technologies were considered as more effective for crime prevention than traditional technologies. More specifically, the respondents perceived the situation of traditional CCTV recordings being watched by security guards as an ineffective surveillance measure since they considered it rather likely that a human loses concentration or is easily distracted:

> "*When I imagine some almost fallen asleep security guard who has to watch thirty screens at once and then he has to go to the toilet or eat a sandwich now and then, well, I do not know if he will see the right thing right on time*" *(P4-III).*

Regarding the deterrent effect of smart technologies, few participants expected surveillance to possibly discourage certain individuals from committing a crime. With a particular emphasis on video-

surveillance, it appears that participants strongly believed that a criminal's intention would not be altered by the mere presence of technological measures: "*If someone wants to kill someone, I would not believe a camera would stop him*" (P2-I).

5.3 Security – Privacy Trade-Offs

5.3.1 Acceptance of Technological Surveillance

In order to gauge the participants' perceptions vis-à-vis the security-privacy trade off, as well as their attitudes towards a number of specific smart technologies, a hypothetical scenario was presented to the group. In brief, this scenario depicted the introduction of a number of smart technologies including smart CCTV, automated number plate recognition (ANPR), sound sensors, the collection of various biometric data (fingerprinting, iris scanning and DNA sample) and electronic tagging. The scenario and two variations of the scenario depicted how these surveillance technologies were introduced by the state following different levels of threat experienced by the citizens[4].

When discussing the scenario, though reactions were somewhat varied, in general there was a tendency for participants to react in a rather rational manner by showing their consideration of different aspects, including the pros and cons of extensive surveillance in the case of an increase in violence and crime. On the one hand, participants seemed to welcome increased video-surveillance in public places to a certain degree, expecting the use of cameras to reduce criminality through a deterrent effect. On the other hand, most participants showed a hostile attitude towards biometric technologies, sound sensors and electronic tagging, since these technologies made the majority of participants feel "*insecure*" (P9-III) and "*scared*" (P1-II). With the exception of CCTV systems, it appears that the intensification of surveillance measures and, accordingly, an increased disclosure of citizens' personal data, were perceived by the participants as representing a threat to citizens' safety, instead of enhancing it: "*I would simply be afraid! I think that is really scary that one would know simply everything about me, I would never feel safe in my life*" (P2-I).

The vulnerability and insecurity conveyed by the respondents with regards to smart surveillance appeared to stem from different factors. Firstly, participants criticised the lack of choice for citizens to decide whether they wanted to be surveilled and also whether they wanted to share their data; they thus perceived this scenario as something that citizens would have been coerced into. Additionally, it appeared that participants perceived these *"repressive"* (P8-II) measures as restricting their freedom; as one participant stated, *"every additional system limits me more*" (P1-II).The participants also argued that the introduction of such extensive surveillance would violate their privacy: "*That would be a too intense infringement of privacy*" (P1-I).

In addition to the above-mentioned concerns vis-à-vis coercion, freedom and privacy, other threats were discussed, including the increased possibility of data theft as well as the misuse of surveillance

[4] The full scenario can be found in Appendix B Item 5.

data. Additionally, a main threat discussed by the respondents in relation to the use of smart surveillance was the increased possibility of misinterpretation by the automatised systems. As a case in point, one participant discussed this in relation to sound sensors:

> *"[…] Cause it happens that one gets a bit louder just for fun, and I would be afraid the police officers would appear next to me immediately. I would be rather afraid to accidently do something wrong instead of feeling safer" (P5-I).*

In particular, the participants showed their concern that this would result in a restriction of individuals' behaviour since they would exercise more caution in order to avoid undesirable situations from occurring. Moreover, it appears that the visibility of surveillance measures, especially exposure to video-surveillance, was considered as unpleasant by a minority of participants who felt this as also having an influence on their behaviour: "*I feel being watched, if I am in a place where I see monitoring cameras. I feel affected. Partly I reflect [on] my behaviour, what I do and challenge it all*" (P1-II).

In spite of a marked increase in crime portrayed in the alternative versions of the scenario, participants were still of the opinion that such surveillance measures could not be justified. In general they argued that surveillance could not solve the problem of violence and that security could never be fully guaranteed, with only a minority arguing in favour of an intensification of surveillance measures following an increase in crime.

In line with the above-mentioned reservations, a number of participants doubted and challenged the notion that surveillance was the best solution to reduce or eliminate crime: "*You do not solve that even with the most complicated security systems*" (P2-III). Furthermore, participants questioned the deterrent effect of surveillance; in their opinion, there is no evidence of a decrease in crime rate following the deployment of more surveillance measures. They thus argued for alternative approaches to be taken: "*The focus should rather be on the prevention of crimes. For me, this is a waste of money and resources*" (P8-II). In addition, rather than investing in technology, it was presumed by some that efforts to boost police presence would be more effective not only for the deterrence of crime, but also in order to increase the possibility of intervention.

Participants emphasised the importance of putting the amount of crimes into perspective, because they appeared to consider the increase in surveillance measures – and in turn the consequences on citizen privacy – as unjustifiable in case of an isolated incident: *"How I see it, it would be absolutely exaggerated to tighten up safety measures just because someone went insane"* (P2-II). The predominant opinion appeared to be that, even if criminality and terrorist attacks increase significantly, these measures were not justified but would rather lead to a "*degradation of society*" (P6-I). Furthermore, a number of participants perceived that the notion that technological surveillance provides protection and safety to citizens could serve as a pretext for the introduction of surveillance tools which could then be potentially employed for the unjustified monitoring of citizens. Surveillance measures were consequently also seen as a strategy by the state and as a *"tool to suppress*" (P1-III).

As mentioned earlier, when participants were confronted with a significantly increasing crime rate, most participants did not significantly change their opinion since they considered privacy as more important than security, especially since in their opinion, criminality could not be eradicated. Nevertheless, a minority of participants considered an increase in criminality as a factor influencing their tolerance of surveillance measures and in this case professed their readiness to compromise their privacy. The discomfort of being surveilled appeared to become more acceptable as long as crime was prevented and their personal safety increased: "*If all these mentioned devices protect me against violence, I will be happy about it in the end*" (P2-II). In this case, a minority of participants showed their willingness to accept the use of biometric technologies, especially for the sake of crime investigation and the prosecution of criminals.

5.3.2 Perceptions of Different Technologies

In general, different types of surveillance technologies appeared to meet different levels of acceptance. Although CCTV systems appeared to be accepted and even considered as desirable for security purposes, the use of smart CCTV with automatic face recognition (AFR) was perceived as impinging on citizens' privacy. A minority of participants considered sound sensors as acceptable, albeit at the same time they argued that they are inefficient due to the possibility of misinterpreting sounds. Biometric technologies and electronic tagging generally provoked a strong sense of violation of privacy, although electronic tagging appeared to be acceptable in certain circumstances.

The use of CCTV appeared to have gone through a process of normalisation and was not only widely perceived as part of "*life's routine*" (P1-III) but was also accepted by the majority of participants: *"CCTV is at this time quite normal and I fully accept it"* (P7-III). In general, participants' attitudes towards video-surveillance contrasted sharply with their attitudes towards other surveillance tools: "*I think anything that goes beyond video surveillance is hardly acceptable*" (P4-II). In particular, the use of video surveillance in public spaces was widely accepted since its use appeared to contribute to feelings of safety. Moreover, due to privacy reasons, some participants also preferred being monitored by cameras rather than being directly surveilled by law enforcement personnel: "*I do not feel restricted by the general technologies. Filming is okay. Worse is massive police presence or something like that. This curtails my rights" (*P-II). Even the deployment of CCTV in private areas appeared to be partly tolerated by many participants, as long as one was aware of its use and could consequently choose whether to avoid it or not.

In relation to the use of sound sensors for the recognition of screams and noises, most participants perceived such devices as acceptable, mainly due to the belief that they are efficient in terms of facilitating law enforcement intervention. Nevertheless, others argued that employing these devices would amount to *"total nonsense"* (P8-II) since their use could result in wrong conclusions being drawn in certain situations, such as when *"someone screams out of joy or if there are children screaming"* (P3-II). Such a consideration made these participants feel uncomfortable: "*I would be afraid to accidently do*

something wrong instead of feeling safer" (P5-I). In addition, one participant argued that criminals could employ sound sensors in order to manipulate police investigations by for instance deliberately using a recorded voice or a mobile phone conversation to fool the sensor and to throw suspicion onto someone else.

In contrast to the above attitudes towards video-surveillance and sound sensors, biometric technologies and electronic tagging provoked a strong negative reaction among a clear majority of participants: "*I could never support this. I guess, I would leave the country [...] I do not want to live under such conditions*" (P3-I). The collection of citizen's DNA and fingerprints was seen as a restriction to individual freedom and as an infringement on privacy. Participants were also concerned that such data collection would be highly subject to misuse and theft. Another reason for the specific rejection of the use of DNA data was because participants related it to health data and therefore the idea of such disclosure made participants feel extremely vulnerable. In general, it appears that most participants agreed upon an exclusive collection of DNA data solely for criminals, as opposed to all citizens.

In relation to electronic tagging and RFID, their use was considered as "*absurd*" (P2-III) for 'normal' citizens, and as extremely intrusive, except for criminals and older people who had to be monitored for their own safety: "*Like when granny runs around in the zoo, you can actually find her again*" (P8-II). However, some scepticism was expressed regarding the efficiency of electronic tagging; some argued that old people with dementia required human attention and supervision rather than being solely monitored by an electronic device. Moreover, some participants were of the opinion that criminals would find ways to circumvent surveillance technologies.

Automatic license plate recognition (ANPR) and GPS systems were briefly discussed. Although few opinions were expressed in relation to these two surveillance methods, they were generally considered as useful for law enforcement purposes and as less intrusive than biometric surveillance and electronic tagging.

5.4 Surveillance Laws and Regulations

During the last part of the focus group sessions, issues relating to surveillance laws and regulations were discussed, including citizens' privacy rights with regards to their transparency and effectiveness, the trust participants have in the state, data storage and issues of data sharing between different entities.

5.4.1 A lack of information and transparency of laws

The first issue under discussion was the accessibility and transparency of surveillance laws and regulations. Overall, participants showed a lack of knowledge with regards to the Data Protection Act, which they partly attributed to their own lack of initiative. In relation to this, a major obstacle perceived was the lack of 'understandable' legal information for 'normal' citizens. This point of view appeared to stem from the respondents' perception that only people with a university degree in law were likely to understand the legislation, since they believed such content to be too technical in order to be grasped by individuals who do not have a legal background.

With regards to privacy policies, participants seemed to believe that the general tendency was for people to naively provide their consent:

> *"The individual doesn't know what he consents to, what he signs and accepts. The individual isn't well informed. He assumes that everything is all right, like it can't be bad or so. He underestimates the situation" (P1-I).*

In the opinion of some of the participants, most people failed to question such policies due to the inability to judge whether they are actually legitimate and if the legal jargon is concealing any conditions to their disadvantage:

> "*I often have the problem that when I sign contracts with a Data Privacy Statement, I cannot really judge whether my data is actually safe, or whether there are hidden clauses, which I cannot see with the naked eye and that they can still give my data away*" (P1-II).

Therefore, participants expressed the wish of having access to 'easily understandable' laws, which clearly define which data was allowed to be collected by whom and which data was not necessary to be disclosed when signing a contract. In their opinion, such knowledge would make it easier for citizens to *"recognise infringements"* (P3-I) on their own.

5.4.2 Trust in the state and effectiveness of legislation

The second issue under discussion was the trust participants have in the German state. The opinions of participants were somewhat divided on this; while some perceived that they could trust the state with the protection of their privacy, it appears that the majority of participants had a rather mistrustful

attitude and stated their preference to rely on themselves, for instance by paying attention to which data they shared.

Specifically in relation to whether the current legislation is effective or not, some participants believed that regardless of the restrictions set by laws, their data was nevertheless still shared with third parties: "*I think the data is just passed on, with no consideration of data protection laws*" (P9-III). Therefore, it was argued that more resolve should be put into protecting citizen's data, such as stepping up enforcement efforts. In addition, the legislation was considered as being reactive: "*I think the data protection is lagging behind, because it is only reacting, it is not foreseeing how to protect from future measures*" (P1-III).

5.4.3 Length of data storage and accessibility

Participants were also asked about their opinions on the length of storage for surveillance data and the restrictions to its accessibility. In general, the participants were also in favour of better public education about what happened with their data, where it was stored and for how long. Participants specifically expressed their insecurity regarding data storage, particularly in relation to the management of, and access to the data, both at present as well as in the future:

> "*What gets more and more precarious is the administration of the data. The data is saved on disks which makes them usable for decades. There may be laws against this nowadays, but what will it be in 10 years?"* (P10-III)

In addition, the risk that stored data could be misappropriated or misused was mentioned by participants: *"Once stored, this is data that can be easily abused*" (P1-II). This was especially the case with DNA data and fingerprints; specifically in relation to these, some participants argued that there exists a high probability that criminals would steal peoples' biometric data in order falsify evidence after committing a crime.

When discussing the length of data storage, participants' opinions about the ideal time period were rather divided; while some participants believed storage length to be irrelevant, others were convinced that a minimum storage time was essential in order to minimise the impact on citizens' privacy and the risk of misuse. Consequently, specifically referring to CCTV recordings, participants expressed their preference for such data to be stored only for a couple of days, and if within this limited period of time no criminal event had been recorded, the record should be deleted in order to respect citizens' 'right to be forgotten'. Nevertheless, specifically in relation to the data of criminals, most participants agreed upon the data to be kept for a longer period of time.

5.4.4 Data sharing between different actors

In general, participants appeared to be in favour of data sharing amongst state authorities, however, not with the complete absence of barriers between the databases, and only as long as access to data was restricted. In addition, many participants expressed the wish to be asked for their consent prior to their data being passed on, in order to know when or for what reason it happened and with whom it was shared: "*I am in favour of using a declaration of consent before your data is shared, because at this point, it is all about trust*" (P4-II).

Nevertheless, when debating the data of criminals and other data pertinent for law enforcement purposes, most participants agreed upon unrestricted access as well as unlimited sharing without the necessary permission for the state and secret services. It appears that this was perceived as increasing safety and security, as well as facilitating communication between entities. A more efficient and faster communication of data was also considered as advantageous and convenient vis-à-vis the sharing of citizen data among state authorities. In addition, participants were also in favour of better communication between state agencies in order to detect the abuse of social benefits, in which case even the sharing of data on an international basis was tolerated.

On a last note, the idea of having their data shared between different private actors made the majority of participants feel very uncomfortable, due to their belief that companies appeared to profit highly from citizens' data. Thus, in relation to this, the majority of participants believed that regulations should be stricter.

6. Conclusion

Throughout the different focus groups, the German participants indicated a high awareness that individual citizens are indeed the subjects of surveillance in the main spaces considered during the discussion. In general, it appears that surveillance by CCTV in public and border spaces has undergone a process of normalisation and is widely accepted for security-related purposes. Moreover, in a commercial context, most participants considered the monitoring of personal data for marketing purposes as generally acceptable, albeit in certain cases some respondents expressed their reservations towards this type of surveillance. On the other hand, in relation to the use of smart phones and online services, the participants were uneasy with the multitude of possibilities of extensive surveillance in this context.

In relation to the massive integration of data, participants' reactions were generally negative, albeit upon discussion, it appears that the acceptance of dataveillance was contingent on several criteria including the type of data collected. In general it appears that most participants objected to sharing more than what they considered as basic personal information. With regards to the acceptance of technologically-mediated surveillance for security-purposes, it appears that while video-surveillance appeared to be widely accepted, the use of smart surveillance, in particular biometric technologies, was perceived as particularly intrusive and unacceptable.

Overall, a number of participants expressed their mistrust in relation to the use of smart technologies. Firstly, they appeared to be particularly concerned with regards to an automatic decision-making process, fearing that this could possibly result in misinterpretations and erroneous conclusions. Other concerns included the risk of misuse of personal data, especially vis-à-vis biometric data, and the fear that extreme surveillance could result in the control of citizens by the state. In addition to these perceived risks, doubts were raised by most participants in relation to whether surveillance measures actually provide a viable solution for the reduction or elimination of crime, which made it difficult for participants to justify their extensive use. Very few participants were in fact willing to sacrifice their privacy for the sake of increased safety in a context of escalating criminality.

In conclusion, the German participants perceived the use of extensive surveillance for the sake of security in a rather cynical manner and appeared to express a deeply rooted resistance to being monitored, not solely due to the belief that this constitutes a violation of privacy but also because of the perception that extreme measures can be used to control and thus restrict individual freedom.

Acknowledgements

This research was carried out as part of SMART (Scalable Measures for Automated Recognition Technologies) a project that was funded by the European Union under the Seventh Framework Programme (2007-2013), Grant Agreement Number 261727.

APPENDIX A – RECRUITMENT QUESTIONNAIRE

Section A

(A1) Gender

- ☐ Male
- ☐ Female

(A2) Age

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45+

(A3) Would you say you live in a

- ☐ Metropolitan city
- ☐ Urban town
- ☐ Rural area

(A4) What is your highest level of education?

- ☐ Primary
- ☐ Secondary
- ☐ Post-secondary
- ☐ Upper secondary
- ☐ Tertiary
- ☐ Post graduate

(A5) What is your occupation?

- ☐ Managerial & professional
- ☐ Supervisory & technical
- ☐ Other white collar
- ☐ Semi-skilled worker
- ☐ Manual worker
- ☐ Student
- ☐ Currently seeking employment
- ☐ Houseperson
- ☐ Retired
- ☐ Long-term unemployed

Section B

(B1) Have you travelled by air during the past year (both domestic and international flights)?

- ☐ Yes
- ☐ No

(B2) Have you crossed a border checkpoint during the last year?

- ☐ Yes
- ☐ No

(B3) Have you ever been part of a large crowd (such as during a concert, rally or sports event)?

- ☐ Yes
- ☐ No

(B4) Do you drive a vehicle?

- ☐ Yes
- ☐ No

(B5) Which of these following devices do you make use of on a regular basis?

- ☐ Computer
- ☐ Laptop
- ☐ Tablets
- ☐ Mobile phone
- ☐ Smart phone
- ☐ Bluetooth
- ☐ In-built cameras (e.g. those in mobile devices)

(B6) If you make use of the internet, for which purposes do you use it?

- ☐ Social networking
- ☐ Online shopping
- ☐ File sharing
- ☐ To communicate (by e-mail etc.)
- ☐ To search for information
- ☐ To make use of e-services (e.g. internet banking)
- ☐ Other activities (please specify):

(B7) Have you made use of any e-government service (including services related to health care, tax purposes and welfare assistance) to make contact with any government agency during the past year?

- ☐ Yes
- ☐ No

(B8) Have you or are you currently receiving any benefits or grants (such as a stipend, scholarship, pension, unemployment benefits etc) from the government?

- ☐ **Yes**
- ☐ **No**

(B9) *Have you given your personal information to a commercial business (local and online) during the past year?*

- ☐ Yes
- ☐ No

(B10) Which of the following personal credentials do you make use of?

- ☐ Identity card
- ☐ Driving licence
- ☐ Passport
- ☐ Payment cards (e.g. credit, debit cards)
- ☐ Store / loyalty card

APPENDIX B

DISCUSSION GUIDELINES (ENGLISH)

Introduction	Briefing
Welcome of participants - *Greeting participants* - *Provision of name tags* - *Signing of consent forms*	*Welcome the participants as soon as they come in. Assign them a seat and provide them with a name tag.* *Distribute the consent form to the participants and ask them to read and sign the form before the start of the focus group. This is important in order to ensure that the participants understand what they have agreed to do.*
Introduction [about 10 min] - *Thank you* - *Introduction of facilitating team* - *Purpose* - *Confidentiality* - *Duration* - *Ground rules for the group* - *Brief introduction of participants*	**Welcome to this focus group and thank you for agreeing to participate in this session. We appreciate that you took this time out of your busy schedule to participate in this project and your involvement is highly valued.** **My name is _____ and I will be facilitating the group discussion. I will be assisted by _____ my co-moderator, who will be taking notes and recording our discussion.** *Introduce any other colleagues who might also be present* **Our session will take between an hour and a half to two hours and since we will be tape recording the discussion, I would kindly ask you to speak in a clear voice; your opinions and thoughts are very important for this research, and we do not want to miss any of your comments.** **As previously mentioned when you were originally contacted to participate in this discussion, this focus group is on the topic of Technology and Privacy, and it is being conducted as part of the SMART Project, which is co-funded by the European Union. For those of you who wish to know more about the SMART Project, kindly let us know and we will proceed to give you more information at the conclusion of the focus group.** *At this stage it is important not to divulge any additional details on the content of the focus group in order to avoid influencing and biasing the ensuing discussion.* **As we already informed you when you read and signed the consent form, everything that will be recorded during this session will be kept confidential and your identity will remain anonymous. This means that your comments will be shared only by those involved in this study and used in scientific publications related to this study, and they will be anonymised before being reported. Hence, the information which will be included in the report will not in any way identify you as a**

	participant. In order to do this, each of you will be assigned a number, and it is this number that will be used in the report. **I also want to make sure that everyone in the group is comfortable enough to share their opinions. To make this possible, I would like to ask everyone present to follow these ground rules:** ▪ **We would like to hear from everyone in the group - we are interested in everyone's opinion** ▪ **There are no right or wrong answers so let us agree to respect each other's opinions** ▪ **Please make sure that your mobile phones are on silent so that the discussion will not get interrupted** ▪ **It is important that comments are made one at a time, since each participant's opinion is important. So let us agree to not speak at the same time, otherwise it will be difficult for us to capture everything that is said during the discussion** ▪ **Let's agree as a group to respect each other's confidentiality so that everyone feels more comfortable in speaking openly.** **If there is anyone who would like to suggest any other ground rules feel free to put your suggestions forward to the group.** **Does anyone have any questions before we start?** **Ok so let me start off by asking you to briefly introduce yourselves to the group without revealing private information. Let's do a round where you tell us your name and maybe something about you. I will start the round myself... *(carry out a brief personal introduction)*** *Running Total: 10 mi*
Objectives	**Discussion items and exercises**
Word association exercise **[About 5mins]** - *Word-association game serving as an ice-breaker* - *Establish top of mind associations with the key themes* - *Start off the group*	***Item 1*** **First up, we will carry out a short game: I will read out a word and I would like you to say the first couple of things that come to mind when you hear the word. Let's try an example first: What is the first thing that comes to mind if I say the word "*food*"? Preferably, try to think about single words or short phrases, avoiding lengthy descriptions.** *Read Out (one at a time):* *Technology, privacy, national security, personal information, personal*

discussion	*safety* ***Running Total: 15min***
Discussion on everyday experiences related to surveillance **[20min]** *- To explore participants' experience with surveillance & how they perceive it* *- To explore participants' awareness and knowledge of the different surveillance technologies*	***Item 2*** **Let's talk about something else. I want you to think about instances during which you feel that either you or your actions are being observed as well as any instances during which you are aware that information about you is being collected. Let's start by thinking about activities you would usually undertake in your everyday life. Let us take the following situations as examples of this.** **Scenario 1: Supermarket** ***As a first example we can take a shopping trip at your usual supermarket. Can you share your thoughts on this?*** **Scenario 2: Travelling** ***Let's move on to another situation, this time related to travelling. What about when you travel by air?*** **Scenario 3: Public place (e.g. museum, stadium)** ***Now imagine that you are visiting a public place, such as a museum or attending an event such as a sports match or a concert. What kind of activities do you think would be recorded?*** **Scenario 4: Mobile devices** **Let us discuss just one final example. Think about the times you use your mobile phone. What do you think is being recorded in this case?** *For each item, and where relevant, probe in detail to explore the following:* ***1. <u>How</u> is the information being collected:*** ***a. Which types of technologies do you think are used to collect your personal information?*** ***2. <u>What</u> type of information is being collected:*** ***a. What type of personal information do you think is being collected?***
Aims: *1. Explore the participants' awareness and knowledge of the technologies* *2. Explore the participants'*	

experience of being monitored in their many roles *3. Explore the participants' understanding of where their information is ending up*	***3. <u>Who</u> is collecting the information:*** ***a. Who do you think is responsible for collecting and recording your personal information?*** ***b. Where do you think your personal information will end up?*** ***4. <u>Why</u> the information is being recorded, collected and stored:*** ***a. Why do you think your personal information is being recorded and collected?*** ***b. In what ways do you think your personal information will be used?*** ***Running Total: 35min***
Presentation of cards depicting different technologies and applications [10mins] *To expose participants to a selection of relevant SMART technologies & applications in order to enable a better understanding and hence to facilitate the discussion.*	***Item 3*** *Present the following three cards (each depicting a group of different technologies and applications) to the group. The cards will include the following depictions:* ***Card 1 – Person or event recognition & tracking technologies**: Automated moving of closed circuit television (CCTV) cameras; Automatic number plate reader (ANPR) or automatic vehicle number identification (AVNI); and tracking devices such as mobile phone tracking and RFID* ***Card 2 - Biometrics**: Biometric technologies including fingerprint and iris scanning; and automatic facial recognition (AFR)* ***Card 3 - Object and product detection devices**: Knife arches (portal) and X-ray devices* ***Running total: 40min***
Presentation of MIMSI scenario to participants **[30mins]** - *To explore participants' understanding of*	***Item 4*** *Present the following hypothetical scenario to the group. A recording of the phone conversation can be prepared beforehand and presented to the group.* ***Phone conversation with the Customer Care Agent at the main branch of the Public Employment Service***

the implications of MIMSI

- *To explore participants' feelings, beliefs and attitudes vis-à-vis the sharing of personal information*

***Customer Care Agent**: Good morning this is Sharon speaking, how are you Mr. Brown? We were expecting your call after your work contract ended over a month ago.*

***Mr. Brown**: Erm...yes in fact that's why I'm calling...*

***Customer Care Agent**: Well, I'm actually not surprised you called now...how was your holiday in Cyprus? I am sure your wife and kids enjoyed the resort you were staying in...*

***Mr. Brown**: Yes it was a lovely holiday...and how do you know all this?*

***Customer Care Agent**: Well, it is in the system, Mr. Brown....obviously. Anyways, better get a head start on finding a new job...what with the cost of your family holiday and your car payment coming up soon...not to mention your VISA payment on the 22nd of this month...*

***Mr. Brown**: Is this also in your system?*

***Customer Care Agent**: Yes, of course Mr. Brown. By the way, good choice on the book you bought online...I read it myself and it gave me some really good tips...*

***Mr. Brown**: Hmmm...ok...regarding this new job seeker service, do I need to provide an updated photo of myself?*

***Customer Care Agent**: No Mr. Brown, that is already taken care of, of course! We have plenty of recent photos in our system. Which reminds me...lovely suntan you got on your holiday! Must have been beautiful weather! Before I forget, regarding the photo, do you prefer one with your glasses or one without?*

***Mr. Brown**: Oh...well....without is fine...so about my registration, can we set up an appointment for sometime next week?*

***Customer Care Agent**: Let me check our system...what about Wednesday at noon? Oh wait a second! I just noticed that you have a doctor's appointment scheduled right at that time. And I'm sure you don't want to miss that since monitoring your cholesterol level is surely important! How about Thursday first thing in the morning at 9am?*

***Mr. Brown**: Thursday morning will be fine...do I need to bring any documentation with me?*

***Customer Care Agent**: No Mr. Brown, we already have all the information we need in our system.*

***Mr. Brown**: I'm sure...*

***Customer Care Agent**: Thank you for calling Mr. Brown and we will see you next week. By the way, enjoy your cappuccino at Cafe Ole'...*

***Mr. Brown**: I am...goodbye...*

Aims

After presenting the previous scenario to the group, probe in-depth to explore the following:

1. Participants' first reactions including:

Possibility / impossibility of scenario

1a. How would you feel if this happened to you?

(Also probe to establish the degree of control / helplessness felt by the participants in such a hypothetical scenario)

1b. How would you react if this happened to you? What would you do?

Acceptability / unacceptability of scenario

1c. Is such a scenario <u>possible / impossible</u>?

1d. Is such a scenario <u>acceptable / unacceptable</u>?

2. Participants' beliefs and attitudes on how technology affects or might affect their privacy

2a. To what extent do you think that "<u>stand alone</u>" (individual technologies) affect your privacy?

2b. To what extent do you think that "<u>smart technologies</u>" i.e. those which process data in an <u>automatic</u> (or semi-automatic) manner affect your privacy?

3. Participants' beliefs and attitudes in terms of the type of information such as: Medical & financial data; photos and location.

3a. What type of personal information do you find <u>acceptable</u> to being collected, used and / or shared?

3b. What type of personal information would you <u>object</u> to being collected, used and / or shared?

4. Participants' beliefs and attitudes on the collection, usage and sharing of personal information with third parties.

4a. What do you think about having your personal information collected, used and shared by the <u>state</u>?

4b. What do you think about having your personal information collected, used and shared by <u>private entities</u> (such as commercial ones)?

5. Participants' beliefs and attitudes

5a. Do you think there are any <u>benefits</u> to having your actions and behaviour monitored?

on the benefits and drawbacks of being monitored

5b. Do you think there are any <u>drawbacks</u> to having your actions and behaviour monitored?

Running Total: 1 hour 15min

Reactions to scenarios

[About 20mins]

- *To stimulate a debate in order to explore the participants' perceptions of the "security vs. privacy trade-off".*
- *Here, the discussion should not focus on whether these technologies will increase security - this should be taken as a given. The discussion should mainly centre on whether these technologies effect privacy and hence revolve around the security - privacy trade-off*

Item 5

During the next exercise, we will be discussing the following hypothetical scenario. Imagine the following scenario:

Due to an significant increase in <u>*violent crimes*</u> in the capital city, including <u>*a spate of kidnappings and murders which seem random and unconnected*</u>, the state has decided to introduce CCTV surveillance in every public space, both those publicly owned (such as subways, public gardens and public conveniences) as well as those privately owned (such as shops, malls and taxis) which will enable automated face-recognition. In addition, all the cars passing through the main check points will have their number plates recorded. There are also plans to install sensors in all public areas which are able to detect loud noises such as in the case of someone screaming. All citizens will be required to have their DNA and fingerprints collected, and their iris scanned. The state has also decided that all citizens who are identified as presenting a possible risk to others should be electronically tagged to monitor and track their movements. For their safety, elderly people and children up to the age of 12 years will also be electronically tagged. All the data from these different technologies will be stored in linked databases administered by the police, who will be notified automatically should there be a cause for alarm and risk to any citizen.

Tell the participants to imagine the above scenario however with the following variations:

Variation 1: Even though a significant increase in violent crime is taking place throughout the majority of neighbouring cities, the city you reside in is not experiencing any increase in crime. However the state still decides to introduce the surveillance measures as a precaution.

Variation 2: The entire country has a very low crime rate in general, but the state still decides to introduce the surveillance measures as a precaution after a neighbouring city experienced an isolated incident during which a number of people were gunned down and seriously injured by a man who opened fire in a shopping mall.

During the discussion of the above scenario/variations, probe in detail to explore the following factors and how they might affect the "security vs. privacy trade off":

Aims:

1. Security climate and level of threat

1a. What makes you feel <u>safe</u> in the scenario provided?

1b. What makes you feel <u>vulnerable</u> in the scenario provided?

1c. Would you be willing to sacrifice your privacy if the level of threat was different as in variation 1 and 2 of the scenario?

2. Deployment of specific technologies

2. From the smart technologies depicted in the scenario, i.e.
CCTV with Automated Facial Recognition,
Automatic Number Plate Recognition (ANPR),
Sensors (with the ability to detect loud noises),
Biometric technologies (including fingerprinting) and
Electronic tagging (which uses RFID)

2a. Which technologies do you consider <u>acceptable</u>? Why?

2b. Which technologies do you consider <u>invasive</u> and as a threat to your privacy? Why?

2c. What do you think of these automated (or semi-automated) technolgies whereby the final decision is taken by the system and not by a human operator?

3. Locations of deployment such as:
Airports
Malls
Streets

3a. Which locations do you consider <u>acceptable</u> in relation to being monitored? Why?

3b. Which locations do you consider <u>unacceptable</u> in relation to being monitored?

4. Existence of laws and other safeguards (in relation to the collection, storage and use of data)

4a. What do you think about privacy laws? Do they make you feel <u>protected</u>?

4b. Are there any <u>safeguards</u> or conditions that you would find <u>reassuring</u>?

5. Length of storage of surveillance data

5a. What do you think about the length of storage of surveillance data? Does it make a difference?

	To help you probe, provide the following examples to the participants: - ***Recordings of CCTV*** - ***The location and movement of cars*** - ***The storage of DNA, fingerprints and iris scans*** - ***The location of citizens who pose a risk to others*** - ***The location and movements of elderly people and children*** ***5b. If length of storage makes a difference, what would you consider as an <u>acceptable timeframe</u>?*** ***Running Total: 1 hour 35min***
Brief summary of discussion [5mins] ▪ *Confirm the main points raised* ▪ *Provide a further chance to elaborate on what was said*	***Item 6 – Summing up session*** ***At the end of the focus group, it is helpful to provide a summary of the emerging points. Here you should aim at giving a brief summing up of the themes and issues raised during the discussion. After, you can ask for the following from the participants:*** - ***"How well does that capture what was said here today?"*** - ***"Is there anything we have missed?"*** - ***"Did we cover everything?"*** - ***This brief session will give participants an additional opportunity to express their views and can also be used to elaborate on topics raised but not pursued at the time.*** ***Running Total: 1 hour 40 min***
Conclusion of focus group **[5mins]** ▪ ***Thank the participants*** ▪ ***Hand out the reimbursement*** ▪ ***Give information on SMART***	***Item 7 –Closure*** **With this last exercise our discussion has come to an end. May we take this opportunity to once again thank you for joining us and for sharing your opinions, experiences and thoughts.** ***At this point, hand out the reimbursements to the participants and inform the participants about the next steps.*** ***Give out more information about the SMART to the participants requesting such information.*** ***Total: 1 hour and 45 min***

APPENDIX C – DISCUSSION GUIDELINES (GERMAN)

Einführung	Einweisung
Begrüßung der Teilnehmer - *Teilnehmer begrüßen* - *Namenschilder erteilen* - *Einwilligungserklärungen unterschreiben lassen*	*Begrüßen Sie die Teilnehmer sobald Sie eintreten. Weisen Sie ihnen einen Platz zu und händigen Sie ihnen ihr **Namensschild** aus.* *Verteilen Sie die Einwilligungserklärungen an die Teilnehmer und bitten Sie sie diese zu lesen und zu unterschreiben, **bevor** die focus group startet. Dies ist wichtig um sicherzustellen, dass die Teilnehmer verstanden haben, wozu sie sich bereit erklärt haben.*
Einführung [ca. 10 min] - *Danke* - *Vorstellung des Moderationsteams* - *Zweck* - *Vertraulichkeit* - *Dauer* - *Grundregeln für die Gruppe* - *Kurze Vorstellung der Teilnehmer*	**Ich heiße Sie herzlich Willkommen zu dieser Gruppendiskussion und danke Ihnen, dass Sie sich bereit erklärt haben, bei dieser Befragung mitzuwirken.** **FRAGEBÖGEN** **EINWILLIGUNGSERKLÄRUNGEN** **Mein Name ist Agnes Rajkowska und ich werde die Gruppendiskussion moderieren. Ich werde hierbei durch meinen Co-Moderator Walter Hötzendorfer unterstützt, der sich ggf. Notizen machen und unsere Diskussion aufzeichnen wird.** *(Stellen Sie ggf. weitere, ebenfalls anwesende Kollegen vor.)* **Unsere Sitzung wird etwa eineinhalb bis zwei Stunden in Anspruch nehmen. Außerdem möchte ich euch bitten, klar und deutlich zu sprechen; eure Meinungen und Gedanken sind sehr wichtig für diese Untersuchung und wir würden ungern eine Bemerkung verpassen.** **Wie bereits anlässlich unserer ersten Kontaktaufnahme bezüglich eurer Teilnahme an dieser Diskussion erwähnt, beschäftigt sich diese Gruppendiskussion mit dem Thema „Technologie und Privatsphäre“ und findet als Teil des Projektes SMART, das von der Europäischen Kommission co-finanziert wird, statt. Diejenigen, die gerne mehr über das SMART-PROJEKT erfahren möchten, mögen sich bitte im Anschluss zu dieser Diskussion an uns wenden: wir sind gerne bereit, Ihnen weitere Informationen zukommen lassen.** *In dieser Phase ist es wichtig, keine weiteren Details über den Inhalt dieser focus group zu enthüllen, um eine Beeinflussung oder einseitige Betrachtungsweise zu vermeiden.*

Wie wir euch bereits mitgeteilt haben, wird alles, was bei dieser Befragung aufgezeichnet wird, vertraulich behandelt. Eure Identität wird anonym bleiben.

Die Informationen, die in den Abschlussbericht kommen, werden euch in keiner Weise als Teilnehmer identifizierbar machen. Um dies zu gewährleisten, haben wir jedem von euch eine Nummer zugewiesen und es wird diese Nummer sein, die im Abschlussbericht verwendet wird.

Ich würde auch gerne gewährleisten, dass jeder in der Gruppe sich wohl dabei fühlt, seine Meinungen zu äußern. Um dies zu ermöglichen, würde ich alle Anwesenden bitten, die folgenden Grundregeln zu beherzigen:

- **Da wir ein großes Interesse an den Auffassungen eines jeden von euch haben, würden wir auch gerne jeden von euch antworten hören. Gleichwohl seid ihr nicht verpflichtet zu antworten.**

- **Ich kann euch sagen, dass es keine richtigen oder falschen Antworten geben wird. Jeder von euch soll sich außerdem wohl dabei fühlen offen zu sprechen. Dafür ist es wichtig, dass wir die Ansichten eines jeden respektieren**

- **Damit die Diskussion nicht unterbrochen wird, stellt bitte sicher, dass eure Handys auf lautlos gestellt sind.**

- **Da uns jede einzelne Ansicht interessiert, ist es außerdem wichtig, dass auch die Kommentare einzeln und für sich abgegeben werden. Ich würde mich daher gerne mit euch darauf verständigen, dass wir nicht gleichzeitig sprechen, da es ansonsten schwierig für uns werden würde, alles was im Zuge dieser Diskussion geäußert wird, auch einzufangen.**

Wenn ansonsten einer von euch gerne irgendeine weitere Grundregel vorschlagen möchte, dann fühlt euch frei, eure Vorschläge jetzt der Gruppe zu unterbreiten.

Hat irgendjemand von euch noch irgendwelche Fragen, bevor wir starten?

In Ordnung, dann lasst uns damit beginnen, dass wir uns einander kurz vorstellen. Ich fange dann mal mit meiner Person an. Ich heiße Agnes Rajkowska und arbeite beim Projekt SMART mit. *(Nun zu meinem Co-Moderator..)*

Gesamtlaufzeit: 10 min

Zielen	Diskussionsthemen und Aufgaben

Wort-Assoziationsübung **[Ca. 5mins]** - *Wort-Assoziationsspiel dient als Aufwärmer* - *Vorrangige Assoziationen mit den Schlüsselthemen aufbauen* - *Diskussion starten*	***Item 1*** **Beginnen wollen wir mit einer Assoziationsübung: Ich werde ein Wort vorlesen und ich möchte euch bitten, die ersten paar Dinge zu sagen, die euch in den Sinn kommen, wenn ihr das Wort hört.** **Versucht nach Möglichkeit an einzelne Worte oder kurze Phrasen anstelle von längeren Beschreibungen zu denken.** **Lasst uns zunächst ein Beispiel ausprobieren:** **Was ist das erste, das euch in den Sinn kommt, wenn ich das Wort "Essen" sage?** **Gut. Dann wollen wir beginnen.** *Lesen Sie (einzeln) vor:* *Technologie, Privatsphäre, Nationale Sicherheit, Personenbezogene Daten, persönliche Sicherheit* *Gesamtlaufzeit: 15min*
Diskussion zu Alltagserfahrung mit Überwachung **[20min]** - *Erkunden, welche Erfahrungen die Teilnehmer mit Überwachung haben und wie sie diese wahrnehmen* - *Erkunden, inwiefern Teilnehmer sich der verschiedenen Überwachungstechnologien gewahr sind und was sie darüber wissen*	***Item 2*** **Lasst uns über etwas anderes sprechen. Ich möchte nun mit euch über Szenarien nachdenken, von denen ihr glaubt, dass ihr in irgendeiner Weise überwacht bzw. dass hierbei Informationen über euch gesammelt werden.** **Lasst uns die folgenden alltäglichen Szenarien als Beispiele dafür heranziehen.** **Szenario 1: Supermarkt - Als erstes Beispiel möche ich, dass ihr an einen Einkauf bei eurem örtlichen Supermarkt denkt. Könnt ihr uns eure Gedanken hierzu mitteilen? Glaubt ihr, dass Sie dabei überwacht werden bzw. Informationen von euch gesammelt werden? Falls „ja" wie und durch wen werden möglicherweise Information gesammelt? Welche Information werden gesammelt und warum werden diese möglicherweise gesammelt?** **Szenario 2: Reisen - Lasst uns bei gleichbleibender Fragestellung mit einer anderen Situation fortfahren, diesmal reisebezogen. Wie ist das, wenn ihr mit einem Flugzeug reist? Werdet ihr hierbei überwacht bzw. werden hierbei Informationen über euch gesammelt? Durch wen und wie? Warum werden diese Informationen gesammelt?** **Szenario 3: Öffentlicher Raum (e.g. Museum, Stadion) - Stellt euch nun vor, dass ihr eine öffentliche Einrichtung besucht, etwa ein Museum, oder dass ihr zu einer Veranstaltung wie einem Fußballspiel oder einem Konzert geht. Werdet ihr hierbei überwacht? Was wird möglicherweise überwacht? Wer überwacht euch und zu welchem**

Zweck?

Szenario 4: Mobile Endgeräte wie zum Beispiel Mobiltelefone - Lasst uns noch ein letztes Beispiel besprechen. Denkt über die Gelegenheiten nach, anlässlich derer ihr euer Handy benutzt. Was glaubt ihr wird in diesem Fall aufgezeichnet und wozu werden diese Informationen aufgezeichnet?

Ziele:

1. Erkunden, inwiefern Teilnehmer sich der verschiedenen Überwachungstechnologien gewahr sind und was sie darüber wissen

2. Erkunden, welche Erfahrungen die Teilnehmer mit Überwachung in ihren verschiedenen Rollen haben,
3. Erkunden, inwiefern die Teilnehmer verstehen, wohin ihre Daten gelangen?

4. Kennenlernen der Ansichten der Teilnehmer, warum ihre Handlungen und ihr Verhalten beobachtet, überwacht und gesammelt werden.

Hinsichtlich jeden Themas, und soweit relevant, fragen Sie nach, um die folgenden Details herauszuarbeiten:

1. ***Wie wird die Information gesammelt:***
    a. ***Welche Arten von Technologien werden Ihrer Meinung nach verwendet, um Ihrer persönlichen Informationen zu sammeln?***

2. ***Welche Art Informationen wird gesammelt:***
    a. ***Welche Art persönlicher Informationen wird Ihrer Meinung nach gesammelt?***

3. ***Wer erhebt diese Informationen:***
    a. ***Wer ist Ihres Erachtens verantwortlich für die Erhebung und Aufzeichnung Ihrer personenbezogenen Informationen?***

    b. ***Was denken Sie, wohin Ihre personenbezogenen Informationen letztlich gelangen werden?***

4. ***Warum werden diese Informationen aufgezeichnet, gesammelt und gespeichert:***

    a. ***Warum denken Sie werden Ihre persönlichen Informationen gesammelt und aufgezeichnet?***

    b. ***Auf welche Arten werden Ihrer Meinung nach Ihre persönlichen Informationen genutzt werden?***

Gesamtlaufzeit: 35min

Präsentation der Karten, welche verschiedene Technologien und Anwendungen zeigen

Item 3

Mein Co-Moderator Walter wird euch nun die verschiedenen neuartigen Überwachungstechnologien erläutern.

Zeigen Sie die folgenden drei Karten (von denen jede eine Gruppe unterschiedlicher Technologien und Anwendungen abbildet) der

[10mins] *Den Teilnehmern eine Auswahl von relevanten SMART Technologien und Anwendungen vorstellen, um sie in die Lage zu versetzen, diese besser zu verstehen und so die Diskussion zu vereinfachen.*	*Gruppe. Die Karten werden die folgenden Abbildungen enthalten:* ***Karte 1 – Technologien zur Erkennung und Ortung von Personen und Ereignissen**: Automatisches Bewegen von Überwachungskameras; Automatische Nummernschilderkennung oder Automatische Fahrzeugnummernerkennung; sowie Ortung von Geräten wie Handy-Ortung oder RFID.* ***Karte 2 – Biometrische Systeme**: Biometrische Technologien einschließlich Fingerabdrucks- und Iris-Scannern; sowie automatische Gesichtserkennung* ***Karte 3 – Technologien zu Erkennung von Objekten und Produkten: Sog. "**Knife Arches" (Portalförmige Metalldetektoren z.B. an Flughäfen) und Röntgengeräte.* *Gesamtlaufzeit: 40min*

Präsentation eines MIMSI Szenarios gegenüber den Teilnehmern

[30mins]

- *Erkunden, inwieweit die Teilnehmer die Implikationen von MIMSI erfassen*
- *Gefühle, Auffassungen und Haltung der Teilnehmer gegenüber der Übermittlung personenbezogener Daten erkunden*

Item 4

Nun werden wir euch ein hypothetisches Szenario vorstellen. Dabei handelt es sich um ein Telefonat eines Herrn Braun mit einer Kundenbetreuerin des Arbeitsmarktservices, die wir Frau Schmidt nennen wollen. Ich werde die Rolle der Kundenbetreuerin Schmidt und Walter wird die Rolle des Kunden Braun übernehmen.

Stellen Sie der Gruppe das folgende, hypothetische Szenario vor. Es kann auch eine Aufzeichnung dieser telephonischen Unterhaltung vorbereitet und der Gruppe präsentiert werden.

Telephonat mit dem Kundenbetreuer bei der Zentralstelle der Bundesagentur für Arbeit

***Kundenbetreuer**: Guten Morgen, Schmidt hier. Wie geht es Ihnen, Herr Braun? Wir hatten eigentlich schon mit Ihrem Anruf gerechnet, nachdem Ihr Arbeitsvertrag bereits vor über einem Monat ausgelaufen war...*

***Herr Braun**: Äh, ja, das ist auch genau der Grund warum ich anrufe.*

***Kundenbetreuer**: Nun, es überrascht mich nicht, dass sie erst jetzt anrufen – wie war denn eigentlich Ihr Urlaub auf Zypern? Ihrer Frau und Ihren Kinder hat das Clubhotel bestimmt gefallen, oder?*

***Herr Braun**: Ja, war ein toller Urlaub... und woher wissen Sie all das?*

***Kundenbetreuer**: Nun, hab ich natürlich hier im System, Herr Braun. Wie dem auch sei, Sie sollten sich besser schnell daran machen, einen neuen Job zu finden… denken Sie an die Kosten Ihres Familienurlaubs und die Ratenzahlung für Ihren Wagen… nicht zu vergessen die VISA Abrechnung am 22. …*

***Herr Braun**: Wie, das haben Sie auch alles im System?*

***Kundenbetreuer**: Ja, selbstverständlich. Übrigens, das Buch, das Sie da online gekauft haben: eine gute Wahl! Hab es selbst gelesen und da waren ein paar echt gute Tipps dabei.*

***Herr Braun**: Hmmm...ok..noch mal zu diesem neuen Arbeitsvermittlungsdienst: brauchen Sie ein aktuelles Bild von mir?*

***Kundenbetreuer**: Nein, nein, darum haben wir uns selbstverständlich schon gekümmert! Wir haben jedemenge aktuelle Bilder in unserem System. À propos: sie haben gut Farbe bekommen im Urlaub. Das Wetter muss toll gewesen sein! Ah, bevor ich es vergessen, wegen des Bildes: bevorzugen Sie eines mit oder ohne Brille?*

***Herr Braun**: Oh...ja...also ohne Brille ist prima... also, wegen meiner Registrierung, könnten wir einen Termin für nächste Woche vereinbaren?*

***Kundenbetreuer**: Lassen Sie mich das kurz im System nachschauen…*

wie ist es Mittwoch mittag? Oh, moment, ich sehe gerade, Sie haben da schon einen Arzttermin. Den sollten Sie lieber wahrnehmen, denn Ihren Cholesterinspiegel überprüfen zu lassen ist sicher sinnvoll! Wie wäre es also mit Donnerstag, gleich als erster morgens um 9.00??

***Herr Braun**: Donnerstag morgen passt! Soll ich irgendwelche Dokumente mitbringen?*

***Kundenbetreuer**: Nein danke, Herr Braun, wir haben bereits alle Unterlagen, die wir brauchen, im System.*

***Herr Braun**: Das glaub ich gern…*

***Kundenbetreuer**: Danke für Ihren Anruf, Herr Braun, wir sehen uns dann nächste Woche. Ach, und genießen Sie ihren Cappuccino im Café Olé …*

***Herr Braun**: Das tue ich ... Auf Wiederhören!*

Zu diesem Szenario möchte ich euch nun einige Fragen stellen.

Nachdem Sie das vorstehende Szenario der Gruppe vorgestellt haben, forschen Sie weiter nach, um mehr über die folgenden Punkte zu erfahren:

Ziele
1. Direkte Reaktion der Teilnehmer, einschließlich:

Möglichkeit / Unmöglichkeit der Existenz eines solchen Szenarios

1a. Wie würdet ihr euch fühlen, wenn euch das passiert wäre? *(Forschen Sie auch nach, um den Grad an wahrgenommener Kontrolle / Hilflosigkeit der Teilnehmer in einem solchen hypothetischen Szenario zu eruieren.)*

1b. Wie würdet ihr reagieren, wenn euch das passiert wäre? Was würdet ihr tun?

1c. Hält ihr ein solches Szenario für <u>möglich oder eher unmöglich</u>?

Akzeptabilität / Inakzeptablität eines solchen Szenarios

1d. Wäre ein solches Szenario für euch <u>akzeptabel</u>?

2. Auffassungen und Einstellungen der Teilnehmer zu der Frage, inwiefern Technologie ihre Privatsphäre beeinflusst

2a. Inwiefern beeinträchtigen eurer Meinung nach herkömmliche Überwachungstechnologien eure Privatsphäre?

2b. Inwiefern beeinträchtigen eurer Meinung nach sog. "<u>smarte Technologien</u>", z.B. solche, die Daten <u>automatisch</u> oder halb-automatisch verarbeiten, eure Privatsphäre?

3. Auffassungen und Einstellungen der

3a. Hinsichtlich welcher Arten personenbezogener Informationen findet ihr deren Erhebung, Nutzung und oder deren Weitergabe <u>akzeptabel</u>?

Teilnehmer zu den Informationstypen wie etwa: Gesundheitsdaten, Finanzdaten, Photos und Ort.

3b. Hinsichtlich welcher Arten personenbezogener Informationen würdet ihr <u>Vorbehalte</u> gegen deren Erhebung, Nutzung und oder deren Weitergabe haben?

4. Auffassungen und Einstellungen der Teilnehmer zur Erhebung, Nutzung und Übermittlung von Personenbezogenen Daten an Dritte.

4a. Was denkt ihr über die Erhebung, Nutzung und Weitergabe eurer personenbezogenen Informationen zwischen einzelnen verschiedenen Behörden (wie z.B. vom AMS an das Finanzamt)? Was denkt ihr über die Erhebung, Nutzung und Weitergabe eurer personenbezogenen Informationen zwischen verschiedenen Staaten?

4b. Was denkt ihr über die Erhebung, Nutzung und Weitergabe eurer personenbezogenen Informationen durch <u>Private Stellen</u> (wie etwa Unternehmen)?

5. Auffassungen und Einstellungen der Teilnehmer zu den Vor- und Nachteilen des Überwachtwerdens.

5a. Glaubt ihr, dass es <u>Vorteile</u> haben könnte, eure Handlungen und euer Verhalten zu überwachen?

5b. Glaubt ihr, dass es <u>Nachteile</u> haben könnte, eure Handlungen und euer Verhalten zu überwachen??

Gesamtlaufzeit: 1 Stunde 15min

Reaktion auf Szenarien

[Ca. 20mins]

- *Stimulation einer Debatte, um die Wahrnehmung der Teilnehmer hinsichtlich des Verhältnisses von "Sicherheit vs. Privatsphäre" zu erkunden.*
- *Die Diskussion sollte sich hier nicht darauf konzentrieren, inwiefern diese Technologien die Sicherheit tatsächlich erhöhen – das sollte als gegeben hingenommen werden. Die Diskussion sollte primär im Zentrum die Frage behandeln, ob diese Technologien die Privatsphäre beeinträchtigen und sich daher um das Verhältnis von Sicherheit zu Privatsphäre drehen.*

Item 5

In der nächsten Übung werden wir ein hypothetisches Szenario diskutieren. Stellt euch folgendes Szenario vor:

Aufgrund der erheblichen Zunahme von Gewaltverbrechen in der Hauptstadt, einschließlich einer Flut von Entführungen und Morden, die zufällig und ohne Verbindung zu sein scheinen, hat das Land beschlossen Videoüberwachung in allen öffentlichen Räumen, sowohl solcher, die der öffentlichen Hand gehören (U-Bahnen, Parks, öffentliche Toiletten), als auch solcher, die in Privateigentum stehen (etwa Geschäfte, Einkaufszentren, Taxis), einzurichten, welche eine automatische Gesichtserkennung ermöglichen wird. Daneben werden alle Fahrzeuge, die die Hauptkontrollpunkte passieren, anhand ihrer Nummernschilder registriert. Weiterhin gibt es Pläne, in allen öffentlichen Räumen Sensoren zu installieren, die laute Geräusche, wie etwa Schreie, erkennen können. Alle Bürger werden verpflichtet, Proben Ihrer DNA und Fingerabdrücke abzugeben, sowie die Iris scannen zu lassen. Das Land hat zudem entschieden, dass alle Bürger, die als mögliche Gefahr für andere identifiziert werden, sog. Elektronische Fußfesseln erhalten sollten, um ihre Bewegungen zu überwachen und aufzuzeichnen. Zu eurer eigenen Sicherheit, erhalten ältere Leute und Kinder bis zum Alter von 12 Jahren ebenfalls solche elektronischen Ortungsgeräte. Der gesamte Datenbestand dieser verschiedenen Technologien wird in vernetzten Datenbanken gespeichert, die durch die Polizei verwaltet werden, welche automatisch benachrichtigt wird, sobald ein Grund zur Alarmierung oder ein Risiko für irgendeinen Bürger besteht.

Im Zuge der Diskussion des obigen Szenarios/ der Variationen, forschen Sie im Detail nach um mehr über die folgenden Faktoren und wie sie das Verhältnis "Sicherheit vs. Privatsphäre" beeinflussen:

1a. Was trägt in dem vorgestellten Szenario dazu bei, dass ihr

euch <u>sicher</u> fühlt?

1b. Was trägt in dem vorgestellten Szenario dazu bei, dass ihr euch <u>verletzlich</u> fühlt?

Wandeln wir nun oben genanntes Szenario etwas ab:

Variation 1: Obwohl ein erheblicher Gewaltanstiegt in der Mehrzahl der Nachbarstädte zu verzeichnen ist, erlebt die Stadt, in der ihr lebt, keinen Anstieg der Kriminalität. Das Land entscheidet dennoch, die Überwachungsmaßnahmen als Vorsichtsmaßnahmen einzuführen.

Variation 2: Das gesamte Land hat eine sehr geringe Kriminalitätsrate insgesamt, das Land entscheidet aber dennoch die Einführung der Überwachungsmaßnahmen als Vorsichtsmaßnahme, nachdem in Einer Nachbarstadt (zB St.Pölten) ein einzelner Zwischenfall stattgefunden hatte, bei dem eine Anzahl Menschen niedergeschossen und ernsthaft verletzt wurde durch einen Mann, der in einem Einkaufszentrum das Feuer eröffnet hatte.

Ziele:

1. Sicherheitsklima und Bedrohungslage

2. Nutzung bestimmter Technologien

1c. Wärt ihr bereit eure Privatsphäre herzugeben, wenn die Gefahrenlage anders wäre, wie in Variation 1 und 2 des Szenarios?

2. Ich will nochmal die intelligenten Überwachungstechnologien des zuvor skizzierten Szenarios in Erinnerung rufen. In chronologischer Reihenfolge waren dies:

- ***Überwachungskameras mit automatischer Gesichtserkennung,***
- ***Automatische Nummernschilderkennung,***
- ***Sensoren (mit der Fähigkeit, laute Geräusche zu erkennen),***
- ***Biometrische Verfahren (einschließlich fingerabdrucksbasierte Verfahren)***
- ***und elektronischer Ortung (unter Nutzung von***

	RFID)
	2a. Welche dieser Technologien findet ihr <u>akzeptabel</u>? Warum?
	2b. Welche dieser Technologien empfindet ihr als <u>in die Privatsphäre eingreifend</u> und als Gefahr für diese? Warum?
	2c. Was hält ihr von diesen automatisierten (oder halb-automatisierten) Technologien, bei denen die Letztentscheidung durch das System und nicht durch einen Menschen getroffen wird?
3. Anwendungsorte wie etwa: Flughäfen Einkaufszentren Straßen	***3a. An welchen Orten fändet ihr die Überwachung eurer Person <u>akzeptabel</u>? Warum?***
	3b. An welchen Orten fändet Sie die Überwachung eurer Person <u>inakzeptabel</u>?
4. Existenz von Gesetzen und anderer Datenschutz-Sicherheitsmaßnahmen (in Bezug auf Erhebung, Speicherung und Nutzung von Daten)	***4a. Was hält ihr vom Datenschutzrecht? Fühlt ihr euch dadurch <u>geschützt</u>?***
	4b. Gibt es irgendwelche datenschutzrechtlichen Sicherheitsmaßnahmen oder Bedingungen, die ihr als beruhigend empfinden würdet?
5. Dauer der Speicherung von Überwachungsdaten	***5a. Was denkt ihr bezüglich der Dauer der Speicherung von Überwachungsdaten? Macht die Dauer der Speicherung einen Unterschied?***
	Nennen Sie den Teilnehmern die folgenden Beispiele um das Gewinnen weiterer Erkenntnisse zu unterstützen: - ***Aufnahmen von Überwachungskameras*** - ***Ort und Bewegung von Fahrzeugen*** - ***Speicherung von DNA, Fingerabdrücken und Iris Scans*** - ***Aufenthaltsort von Bürgern, die für andere ein Risiko darstellen*** - ***Aufenthaltsort und Bewegungen älterer Leute und von Kindern***
	5b. Soweit die Dauer der Speicherung einen Unterschied macht, welchen <u>Zeitrahmen</u> fändet ihr <u>akzeptabel</u>?
	Gesamtlaufzeit: 1 Stunde 35min
Ziele	**Zusammenfassung der Session**

Kurze Zusammenfassung der Diskussion [5mins] ▪ *Bestätigung der wesentlichen der angeführten Aspekte* ▪ *Weitere Gelegenheit das Gesagte zu vertiefen*	***Item 6*** ***Am Ende der "focus group" ist es hilfreich, die herausgearbeiteten Punkte zusammenzufassen. Hier sollten Sie darauf abzielen, eine kurze Zusammenfassung der während der Diskussion aufgekommenen Themen und Problematiken zu geben. Danach können Sie die Teilnehmer folgendes fragen:*** - **"Wie gut gibt das wieder, was heute hier gesagt wurde?"** - **"Gibt es etwas, das wir vergessen haben?"** - **"Haben wir alles abgedeckt?"** ***Diese kurze Session wird es Teilnehmer ein weiteres mal ermöglichen, Ihre Ansichten zum Ausdruck zu bringen und kann zudem dafür genutzt werden, Themen, die zur Sprache kamen, aber vorher nicht weiter verfolgt wurden, zu vertiefen.*** ***Gesamtlaufzeit: 1 Stunde 40 min***

Ziele	Verabschiedung
Beendigung der focus group **[5mins]** ▪ ***Den Teilnehmern danken*** ▪ ***Auslagenerstattung*** ▪ ***Weitere Informationen zu SMART***	***Item 7*** **Mit dieser letzten Aufgabe ist unsere Diskussion an ihr Ende gelangt. Lasst uns diese Gelegenheit nutzen, euch ein weiteres Mal dafür zu danken, dass ihr teilgenommen und eure Ansichten, Erfahrungen und Gedanken mit uns geteilt habt.** ***Erstatten Sie nun den Teilnehmern die Auslagen und informieren Sie die Teilnehmer über die nächsten Schritte.*** ***Händigen Sie den Teilnehmern auf Verlangen weitere Informationen zu SMART aus.*** ***Gesamtlaufzeit: 1 Stunde 45 min***

APPENDIX D – DEBRIEFING FORM

SMART WP10 Focus Group De-briefing form	
1. Date	
2. Duration	
3. Facilitating team	Moderator: Co-moderator: Other team members:
4. Group composition 4a. Number of participants 4b. Gender ratio 4c. Age categories	 Participants present: Participant no-shows: Males: Females: 18-24 years: 25-44 years: 45+ years:
5. Overall observations 5a. **Group dynamics:** How would you describe the group dynamics / atmosphere during the session? 5b. **Discussion**: How would you describe the overall flow of the discussion? 5c. **Participants**: Were there any individual participants who stood out? (For instance, participants who might have been particularly talkative, dominant, silent or aggressive)	
6. Content of the discussion 6a. **Themes:** What were some of the most prominent themes and ideas discussed about? Did anything surprising or unexpected emerge (such as new themes and ideas)? 6b. **Missing information:** Specify any content which you feel was overlooked or not	

explored in detail? (E.g. due to lack of time etc.) 6c. **Trouble spots**: Were there any particular questions and/or items which did not lead to the desired information (kindly pinpoint which ones, if any)	
7. Problems or difficulties encountered Did you encounter any difficulties in relation to the following? If yes, kindly explain in detail. 7a. **Organisation and logistics** (For instance those relating to location, venue, any interruptions, reimbursement and refreshments) 7b. **Time management**: Timing of particular items in the discussion guidelines and timing of the overall discussion 7c. **Group facilitation** (For instance whether it was difficult to get the discussion going etc.) 7d. **Focus group tools** (For instance the recording equipment and handouts)	
8. Additional comments	

APPENDIX E – CONSENT FORM

You have been asked to participate in a focus group being conducted as part of the SMART Project, which is co-funded by the European Union. This focus group is being carried out by the *<insert name of institution here>* which is the co-ordinator for the SMART project in *<insert country here>.* The information obtained during this discussion plays a very important part in the research being carried out as part of this international project.

Participation

The focus group discussion will take approximately two hours. Your participation in this group is entirely voluntary and you may stop your participation at any time. You may also refuse to answer any questions with which you are uncomfortable. You may also withdraw your participation from the focus group at any time, and no penalties will be incurred should you withdraw from the study.

Confidentiality and anonymity

The discussion will be recorded however all personal information collected and your responses will be anonymised as soon as reasonably possible. Your name will not be connected to your responses; instead, a number will be utilised for identification purposes. In addition, any information which could potentially make it possible for you to be identified will not be included in any report. Your personal data will be kept confidential and it will only be disclosed to those individuals working on the SMART project on a need-to-know basis and it will not be disclosed to any other individual or third parties unrelated to the SMART project. Your anonymised comments might be used in scientific publications related to this study

Out of respect for each other, we kindly ask that the participants' responses be kept confidential. Nonetheless, we cannot offer any assurance that the participants will keep confidentiality.

Data protection and data security

All personal data collected will be kept secure and no personal data will be kept for longer than necessary for the purposes for which it was collected. Personal data which is no longer required for the purposes of the SMART project will be deleted.

Risks and benefits

No risks are foreseen to the focus group participants. Your participation in this research will most likely not result in any benefit to yourself; however it will assist the researchers concerned in providing valuable information on the topic under study.

Questions about the research

If you wish further information on the SMART Project, you can be given this information when the focus group discussion is concluded.

I confirm that I have read and understood the above information and I agree, out of my own free will and volition, to participate under the stated conditions.

Signature: Date:

APPENDIX F – CODING MAP

1. Surveillance technologies in different spaces

1.1. Commercial space

1.1.1. Awareness of different surveillance methods/technologies

1.1.1.1. Loyalty cards

1.1.1.2. CCTV

1.1.1.3. Financial monitoring

1.1.1.4. RFID-tags

1.1.2. Perceived purposes

1.1.2.1. Collection of personal data

1.1.2.2. Market research

1.1.2.3. Shelf and product organisation

1.1.2.4. Creation of customer databases

1.1.2.5. Tracking of stolen items

1.1.2.6. Theft prevention

1.2. Boundary space

1.2.1. Awareness of different surveillance methods/technologies

1.2.1.1. CCTV

1.2.1.2. Monitoring of personal data

1.2.1.2.1. Passport control

1.2.1.2.2. Loyalty cards e.g. bonus cards

1.2.1.3. Object and product detection

1.2.1.3.1. Physical screening by security agents

1.2.1.3.2. Luggage check

1.2.1.3.3. X-rays

1.2.1.3.4. Body scanners

1.2.2. Perceived purposes

1.2.2.1. Observation of people

1.2.2.2. National security

1.2.2.3. Prevention of crime, terrorism and illegal immigration

1.2.2.4. Tracking of criminals

1.2.2.5. Customs affairs

1.2.2.6. Organisational reasons

1.2.2.7. Marketing and analysis of traveller behaviour

1.3. Common public spaces

1.3.1. Awareness of different surveillance methods/technologies

1.3.1.1. CCTV

1.3.1.2. Law enforcement personnel and security guards

1.3.2. Perceived purposes

1.3.2.1. Deterrence
1.3.2.2. Investigation of crimes
1.3.2.3. Security
1.3.2.4. Commercial reasons
1.3.2.5. Protection of property
1.3.2.6. Prevention of vandalism and theft

1.4. Mobile devices and virtual spaces
1.4.1. Awareness of different surveillance methods/technologies
1.4.1.1. Location tracking via GPS
1.4.1.2. Monitoring of call lists and data traffic
1.4.1.3. Recording of phone call conversations
1.4.2. Perceived purposes
1.4.2.1. Collection of data
1.4.2.2. Criminal investigations and prevention of crime
1.4.2.3. Security

2. Perceptions and attitudes towards smart surveillance and integrated dataveillance

2.1. Feelings
2.1.1. Extreme discomfort
2.1.1.1. Fear
2.1.1.2. Shock
2.1.2. Helplessness and resignation
2.1.2.1. Insecurity
2.1.2.2. Rejection
2.1.3. Indignation and anger
2.1.3.1. Violation of rights
2.1.4. Convenience
2.1.4.1. Efficient service

2.2. Behavioural intentions
2.2.1. Active reactions
2.2.1.1.1. Take independent action and counteract
2.2.2. Take legal action
2.2.2.1. Investigate the legitimacy
2.2.2.2. Confront the state
2.2.2.3. File an organisational complaint
2.2.3. Passive reactions
2.2.3.1. Immediate withdrawal
2.2.3.2. Escape from public exposure

2.3. Beliefs
2.3.1. Likelihood of smart surveillance and integrated dataveillance
2.3.1.1. Technical aspect

2.3.1.1.1. Technological development
2.3.1.1.2. Massive integration of data
2.3.1.2. Legal aspect
2.3.1.2.1. Legal boundaries
2.3.1.2.2. Protection of privacy
2.3.2. Acceptance of smart surveillance and integrated dataveillance
2.3.2.1. Type of data
2.3.2.1.1. Identity card data
2.3.2.1.2. Basic personal details
2.3.2.1.3. Financial and health data
2.3.2.1.4. Beliefs and sexual orientation
2.3.2.2. Purpose and collection
2.3.3. Perceived effectiveness of smart technologies and dataveillance
2.3.3.1. Decision-making capabilities of automated systems
2.3.3.1.1. Misinterpretations
2.3.3.1.2. Inaccuracy
2.3.3.1.3. Wrong conclusions
2.3.3.1.4. Efficiency in crime prevention
2.3.3.2. Human factor
2.3.3.2.1. Discrimination
2.3.3.2.2. Influence by biases
2.3.3.2.3. Distraction
2.3.3.3. Programming for the recognition of behavioural patterns
2.3.3.3.1. Dehumanisation

3. Security-privacy trade-offs

3.1. Acceptance of technological surveillance
3.1.1. Feelings
3.1.1.1. Convenience: Deterrent effect
3.1.1.2. Vulnerability: surveillance produces insecurity
3.1.2. General beliefs
3.1.2.1. Loss of choice of data sharing
3.1.2.2. Restriction of freedom
3.1.2.3. Violation of privacy
3.1.2.4. Threat of data theft and misuse of data
3.1.2.5. Degradation of society
3.1.3. Effectiveness of surveillance
3.1.3.1. Risk of misinterpretation
3.1.3.2. Restriction in behavioural liberty
3.1.3.3. Solution to crime

3.1.3.4. Deterrent effect
3.1.3.5. Possibility of intervention
3.2. Perceptions of different technologies
3.2.1. CCTV
3.2.1.1. Process of normalisation
3.2.1.2. Feeling of safety
3.2.1.3. Objective monitoring
3.2.2. Sound sensors
3.2.2.1. Acceptance
3.2.2.2. Possibility of wrong conclusions
3.2.2.3. Manipulation
3.2.3. Biometric data
3.2.3.1. Restriction to individual freedom
3.2.3.2. Infringement on privacy
3.2.3.3. Misuse and theft
3.2.3.4. Connection to health data
3.2.4. Electronic tagging (RFID) and GPS
3.2.4.1. Impingement of privacy
3.2.4.2. Efficiency
3.2.4.3. Possibility of circumvention by criminals

4. Surveillance laws and regulations

4.1. Feelings and beliefs
4.1.1. A lack of information and transparency
4.1.1.1. Data Protection Act
4.1.1.2. Lack of understandable legal information
4.1.2. Trust in the state and effectiveness of legislation
4.1.2.1. Self-protection
4.1.2.2. More enforcement
4.1.3. Length of data storage and accessibility
4.1.3.1. Public education
4.1.3.2. Risk of misuse
4.1.3.3. Deletion of data after limited time period
4.1.4. Data sharing between different actors
4.1.4.1. Databases of public authorities
4.1.4.2. Consent of citizens before sharing
4.1.4.3. Unrestricted access for data of criminals
4.1.4.4. More efficient and faster communication of data
4.1.4.5. Profit from data sharing